Symantec™ IT Management Suite 7.5 powered by Altiris™ – Administratorhandbuch

Symantec

Symantec™ IT Management Suite 7.5 powered by Altiris™ – Administratorhandbuch

Die in diesem Handbuch beschriebene Software wird unter einer Lizenzvereinbarung zur Verfügung gestellt und darf nur gemäß den Bestimmungen dieser Vereinbarung verwendet werden.

Rechtlicher Hinweis

Copyright © 2013 Symantec Corporation. Alle Rechte vorbehalten.

Symantec, Altiris, the Symantec Logo, and the Checkmark Logo, and any Altiris or Symantec trademarks used in the product are trademarks or registered trademarks of Symantec Corporation or its affiliates in the U.S. and other countries. Other names may be trademarks of their respective owners.

Dieses Symantec-Produkt kann Drittanbietersoftware enthalten, für die Symantec die Rechte der Drittanbieter ("Nicht-Symantec-Programme") anerkennt. Some of the Third Party Programs are available under open source or free software licenses. The License Agreement accompanying the Licensed Software does not alter any rights or obligations you may have under those open source or free software licenses. For more information on the Third Party Programs, please see the Third Party Notice document for this Symantec product that may be available at http://www.symantec.com/about/profile/policies/eulas/, the Third Party Legal Notice Appendix that may be included with this Documentation and/or Third Party Legal Notice ReadMe File that may accompany this Symantec product.

Das in diesem Dokument beschriebene Produkt wird unter Lizenzen vertrieben, die die Nutzung, Vervielfältigung, Verteilung und Dekompilierung/Zurückentwicklung (reverse engineering) einschränken. Ohne vorherige schriftliche Genehmigung der Symantec Corporation oder ihrer Lizenzgeber (falls zutreffend) darf kein Teil dieses Dokuments vervielfältigt werden, unabhängig davon, in welcher Form oder mit welchen Mitteln dies geschieht.

DIE DOKUMENTATION WIRD OHNE MÄNGELGEWÄHR BEREITGESTELLT. ALLE AUSDRÜCKLICHEN UND STILLSCHWEIGENDEN VORAUSSETZUNGEN, DARSTELLUNGEN UND GEWÄHRLEISTUNGEN, EINSCHLIESSLICH DER STILLSCHWEIGENDEN GEWÄHRLEISTUNG DER MARKTGÄNGIGKEIT, EIGNUNG FÜR EINEN BESTIMMTEN ZWECK ODER NICHT-BEEINTRÄCHTIGUNG, SIND AUSGESCHLOSSEN, AUSSER IN DEM UMFANG, IN DEM SOLCHE HAFTUNGSAUSSCHLÜSSE ALS NICHT RECHTSGÜLTIG ANGESEHEN WERDEN. SYMANTEC CORPORATION IST NICHT VERANTWORTLICH FÜR INDIREKTE SCHÄDEN ODER FOLGESCHÄDEN IM ZUSAMMENHANG MIT DER BEREITSTELLUNG ODER VERWENDUNG DIESER DOKUMENTATION. DIE IN DIESER DOKUMENTATION ENTHALTENEN INFORMATIONEN KÖNNEN JEDERZEIT OHNE ANKÜNDIGUNG GEÄNDERT WERDEN.

The Licensed Software and Documentation are deemed to be commercial computer software as defined in FAR 12.212 and subject to restricted rights as defined in FAR Section 52.227-19 "Commercial Computer Software - Restricted Rights" and DFARS 227.7202, "Rights in

Commercial Computer Software or Commercial Computer Software Documentation", as applicable, and any successor regulations. Any use, modification, reproduction release, performance, display or disclosure of the Licensed Software and Documentation by the U.S. Government shall be solely in accordance with the terms of this Agreement.

Symantec Corporation
350 Ellis Street
Mountain View, CA 94043

http://www.symantec.de

Technischer Support

Der technische Support von Symantec unterhält weltweit Supportcenter. Hauptaufgabe des technischen Supports ist es, bestimmte Anfragen zu Produktmerkmalen und -funktionen zu bearbeiten. Daneben erstellt die Gruppe "Technischer Support" Inhalte für unsere Online-Supportdatenbank. Die Gruppe "Technischer Support" arbeitet mit den anderen Funktionsbereichen von Symantec zusammen, um Ihre Fragen zeitnah zu beantworten. So arbeitet diese Gruppe z. B. mit der Produktentwicklung und Symantec Security Response zusammen, um Warnmeldungsdienste und Aktualisierungen der Virendefinitionen zur Verfügung zu stellen.

Die Supportangebote von Symantec umfassen folgende Leistungen:

- Verschiedene Supportoptionen, die Ihnen die Flexibilität bieten, den richtigen Serviceumfang für Unternehmen aller Größen auszuwählen
- Telefon- und/oder webbasierter Support, der schnell reagiert und aktuelle Informationen bietet
- Upgrade-Versicherung, die Software-Upgrades liefert
- Weltweiter Support, der auf Basis regionaler Geschäftsstunden oder auf 24-Stunden-Basis erworben wird
- Erstklassige Serviceangebote, die Kontoverwaltungsservices umfassen

Informationen zu den Supportangeboten von Symantec finden Sie auf unserer Website unter folgender URL:

www.symantec.com/business/support/

Alle Support-Dienste werden in Übereinstimmung mit Ihrer Supportvereinbarung und der zu dem Zeitpunkt geltenden technischen Enterprise-Support-Richtlinie bereitgestellt.

Kontaktieren des technischen Supports

Kunden mit einem aktuellen Supportvertrag können auf Informationen des technischen Supports unter folgender URL zugreifen:

www.symantec.com/de/de/business/support/

Bevor Sie den technischen Support kontaktieren, stellen Sie sicher, dass die Systemanforderungen erfüllt sind, die in Ihrer Produktdokumentation aufgelistet sind. Auch sollten Sie sich an dem Computer befinden, auf dem das Problem aufgetreten ist, falls eine Replizierung des Problems notwendig ist.

Wenn Sie den technischen Support kontaktieren, halten Sie bitte die folgenden Informationen bereit:

- Produktversion
- Hardware-Daten
- Verfügbarer Arbeitsspeicher, Speicherplatz und NIC-Informationen
- Betriebssystem
- Version und Patch-Level
- Netzwerktopologie
- Informationen zu Router, Gateway und IP-Adressen
- Problembeschreibung:
  - Fehlermeldungen und Protokolldateien
  - Fehlerbehebungsmaßnahmen, die vor Kontaktaufnahme mit Symantec durchgeführt wurden
  - Aktuelle Softwarekonfigurationsänderungen und Netzwerkänderungen

Lizenzierung und Registrierung

Wenn Ihr Symantec-Produkt eine Registrierung oder einen Lizenzschlüssel erfordert, besuchen Sie unsere technische Support-Webseite:

www.symantec.com/de/de/business/support/

Kundenservice

Informationen zum Kundenservice finden Sie unter folgender URL:

www.symantec.com/de/de/business/support/

Der Kundenservice kann bei nicht-technischen Fragen helfen. Beispiele:

- Fragen zu Produktlizenzen und -seriennummern
- Aktualisieren persönlicher Angaben wie Anschrift und Name
- Allgemeine Produktinformationen (Funktionen, verfügbare Sprachen, lokale Anbieter)
- Neueste Informationen zu Produkt-Updates und -Upgrades
- Informationen zu Upgrade-Versicherung und Support-Verträgen
- Informationen zum Symantec Buying Program
- Informationen zu den Optionen des technischen Support von Symantec
- Nichttechnische Fragen zu vertriebsvorbereitenden Maßnahmen
- Probleme mit CDs, DVDs oder Handbüchern

Ressourcen zum Supportvertrag

Wenn Sie Symantec bezüglich eines vorhandenen Supportvertrags kontaktieren möchten, wenden Sie sich bitte an das Supportvertragsverwaltungsteam für Ihre Region:

Asien-Pazifik und Japan	customercare_apac@symantec.com
Europa, Nahost und Afrika	semea@symantec.com
Nordamerika und Lateinamerika	supportsolutions@symantec.com

Inhalt

Technischer Support 4

Abschnitt 1 Einführung in die Schlüsselkomponenten von IT Management Suite 22

Kapitel 1 Einführung in Symantec Management-Plattform 23

Info zur Symantec Management-Plattform 23
Neue Funktionen in IT Management Suite 7.5 24
Komponenten der Symantec Management-Plattform 27
Funktionsweise von pcAnywhere Solution 28
Infos zum Hinzufügen von Produkten zur Plattform 29
Weitere Informationen 30

Kapitel 2 Einführung in die Symantec Management Console 33

Info zur Symantec Management Console 33
Info zu Konsolenansichten 35
Info zur Ansicht "Computer" 36
Suchen nach einem Computer und Speichern der Suche als Filter 39
Über die Ansicht "Software" 41
Suchen nach Software und Speichern der Suche 41
Informationen zum Fenster Softwarekatalog 43
Informationen zur Ansicht Jobs/Aufgaben 44
Informationen zur Ansicht Richtlinien 44
Info zu Suchoperatoren 45
Konfigurieren der erweiterten Ansichten 46
Aufrufen der Symantec Management Console 48
Aufrufen der Dokumentation in der Symantec Management Console 50
Aufrufen der Seite "Mein Portal" 51
Zugreifen auf die Startseite von Notification Server Management 51

Anpassen der Symantec Management Console 52
Anpassen des Konsolenmenüs 54
Hinzufügen benutzerdefinierter Aktionen zum Kontextmenü 55
Erstellen und Ändern von Ansichten 57
Hinzufügen neuer Elemente direkt zu einer Ansicht 58
Erstellen und Ändern von Portalseiten 59
Erstellen und Ändern von Web-Parts 62
Speichern der Konsolenelemente als XML-Dateien 63

Abschnitt 2 Einrichten der Symantec Management-Plattform-Server 65

Kapitel 3 Konfigurieren von Notification Server 66

Informationen zum Notification Server 66
Info zum Konfigurieren von Notification Server 67
Konfigurieren von Notification Server-Einstellungen 68
Notification Server-Verarbeitungseinstellungen 69
Einstellungen für E-Mail-Server und -Adresse 73
Einstellungen für die Protokollierung von Statusmeldungen 74
Öffnen der Protokollanzeige 74
Proxy-Server-Einstellungen 75
Einstellungen für Verteilungspunkt-Identifikationsdaten 76
Konfigurieren von Notification Server-Einstellungen mit NS Configurator 77
Konfigurieren von Configuration Management Database 78
Bereinigen der Configuration Management Database 82
Speichern des Ressourcendatenverlaufs in der CMDB 84

Kapitel 4 Konfigurieren der Sicherheit 86

Infos zur Sicherheit der Symantec Management-Plattform 86
Einrichten der Sicherheit für die Symantec Management-Plattform 88
Erstellen und Konfigurieren von Sicherheitsrollen 91
Zuweisen von Privilegien zu einer Sicherheitsrolle 97
Erstellen und Konfigurieren von Benutzerkonten der Symantec Management-Plattform 233
Angeben allgemeiner Details für ein Symantec Management-Plattform-Benutzerkonto 101
Konfigurieren von Identifikationsdaten für ein Symantec Management-Plattform-Benutzerkonto 102
Hinzufügen von Mitgliedern für eine Sicherheitsrolle 105

Zuweisen eines Symantec Management-Plattform-Benutzerkontos zu einer Sicherheitsrolle 106
Hinzufügen von Sicherheitsrollen als Mitglieder anderer Sicherheitsrollen 107
Zuweisen von Sicherheitsberechtigungen zu Ordnern und Elementen 108
Anpassen der Vererbungsregeln für Berechtigungen 109
Vordefinierte Sicherheitsrollen 112
Sicherheitsverwaltungsaufgaben für Symantec Management-Plattform 114
Konfigurieren von Kennwortkomplexitäts- und Sperreinstellungen 115
Freigeben von gesperrten Identifikationsdaten 118
Zugriff auf den Sicherheitsrollenmanager 119
Besitznahme über Ordner oder Elemente 120
Verwalten von Identifikationsdaten 121

Kapitel 5 Konfigurieren von Zeitplänen 123

Verwendung von Zeitplänen durch die Symantec Management-Plattform 123
Komponenten eines Symantec Management-Plattform-Zeitplans 125
Verwalten gemeinsam genutzter Zeitpläne 128
Konfigurieren eines Zeitplans 129
Anzeigen des internen Zeitplankalenders des Notification Servers 130

Kapitel 6 Konfigurieren von Sites und Site Servers 133

Info zu Site Services 133
Info zur Site-Verwaltung 134
Verwalten von Sites 135
Verwalten von Site Servers 137
Manuelles Zuweisen eines Site Server zu einer Site 140
Verwalten manuell zugewiesener Agents 141
Verwalten von Subnetzen 142
Info zum Konfigurieren der Einstellungen für den Site Service 145
Konfigurieren der Package Service-Einstellungen 146
Konfigurieren der Task Service-Einstellungen 146

Kapitel 7 Konfigurieren der Package Server für Linux 148

Info zu Package Server für Linux 148
Info zur Integration von Apache Web Server mit Package Server für Linux 149
Info zur Erkennung von Apache Web Server 150
Konfigurationsanforderungen für Package Server und Apache Web Server 152
Konfigurationsanforderungen von HTTPS und HTTP 153
Package Server-Konfigurationsbeispiel, dass das Haupt-Webverzeichnis für Package Server-Links verwendet 154
Package Server-Konfigurationsbeispiel unter Verwendung eines Alias für Package Server-Links 157

Kapitel 8 Konfigurieren der Hierarchie 160

Info zur Notification Server-Hierarchie 160
Hierarchieanforderungen 162
Implementieren der Notification Server-Hierarchie 163
Erstellen und Verwalten hierarchischer Beziehungen 164
Einrichten einer Hierarchiebeziehung zwischen zwei Notification Server-Computern 168
Konfigurieren der Hierarchiereplikation und Hierarchiereplikationsregeln 170
Einrichten der benutzerdefinierten Hierarchiereplikation 173
Übergehen des Differenzial-Replikationszeitplans für Hierarchien 174
Manuelles Replizieren ausgewählter Daten 175
Einrichten einer Hierarchieautomatisierungsrichtlinie 176
Ausführen eines Hierarchieberichts 177
Aktualisieren von Übersichtsdaten 178

Kapitel 9 Konfigurieren der Replikation 180

Info zu Replikation und Replikationsregeln 180
Replikationsanforderungen 182
Konfigurieren von Replikationsregeln 183

Kapitel 10 Erstmalige Konfiguration 185

Ausüben von Konfigurationsaufgaben bei der Ersteinrichtung 185
Erkennen von Computern 186
Ausführen eines Rollouts für Symantec Management-Agent und -Lösungs-Plugins 189
Agent- und Aufgaben-Einstellungsoptionen 192

Erfassen von Inventardaten 193
Planen des Patch-Managements 195

Abschnitt 3 Erkennen der Ressourcen im Netzwerk 197

Kapitel 11 Erkennen von Windows-Computern 198

Ressourcenerkennungsmethoden 198
Erkennungsmethoden für Windows-Computer 199
Erkennen von Computern mit der Domänen-Ressourcenerkennung 200

Kapitel 12 Importieren von Ressourcen aus Active Directory 205

Info zu Microsoft Active Directory-Import 205
Importieren von Ressourcenzuordnungen 206
Importieren von Ressourcen mit Microsoft Active Directory-Import 207
Erstellen und Ändern von Ressourcenimportregeln 209
Planen von Ressourcenimportregeln 212
Konfigurieren des Zeitplans für Verzeichnissynchronisierung 213
Manuelles Ausführen von Ressourcenimportregeln 214

Kapitel 13 Erkennen von Netzwerkgeräten 216

Info zu Network Discovery 216
Erkennen von Netzwerkgeräten 217
Konfigurieren von Erkennungseinstellungen 218
Erstellen von "Network Discovery"-Aufgaben mithilfe des Assistenten 220
Manuelles Erstellen und Ändern von Network Discovery-Aufgaben 221
Erstellen von Verbindungsprofilen mit Network Discovery 222
Erstellen oder Duplizieren eines Verbindungsprofils 223
Methoden zum Erkennen von Netzwerkgeräten 224
Info zum Auswählen von zu erkennenden Netzwerkbereichen 226
Anzeigen erkannter Geräte in Organisationsansichten 227
Anzeigen von Erkennungsberichten 227
Klassifizieren von SNMP-Geräten 228

Delegieren von Netzwerkerkennungsaufgaben an Nicht-Administratorbenutzer 229
Hinzufügen von Nicht-Administratorbenutzern zu den Sicherheitsrollen für die Ausführung von Netzwerkerkennungsaufgaben 233
Ermöglichen, dass Nicht-Administratorrollen Netzwerkerkennungsaufgaben erstellen oder ausführen können 235
Gewähren von Privilegien zur Erstellung von Identifikationsdaten und Verbindungsprofilen für Nicht-Administratorrollen 238
Erteilen von Zugriff für Nicht-Administrator-Rollen auf das Standardverbindungsprofil 239
Aktivieren der Erstellung und Ausführung von Aufgaben durch andere Rollen als die vordefinierten Sicherheitsrollen mithilfe des Network Discovery-Assistenten 240
Aktivieren des Schreibschutzes für ein Verbindungsprofil 242
Importieren von MIB-Dateien 243

Abschnitt 4 Installieren und Konfigurieren des Symantec Management-Agent 245

Kapitel 14 Einführung in den Symantec Management-Agent 246

Infos zu Symantec Management-Agent 246
Info zu Agent-Registrierung 247

Kapitel 15 Installieren des Symantec Management Agent auf Clientcomputern 248

Methoden für das Installieren des Symantec Management-Agent 248
Installieren des Symantec Management-Agent unter Windows 250
Anforderungen für das Installieren des Symantec Management-Agent unter Windows 252
Erstellen einer Agent-Registrierungsrichtlinie 253
Angeben des Symantec Management-Agent für Windows-Installationseinstellungen 256
Installieren des Symantec Management-Agent für Windows mit einer manuellen Push-Installation 256
Installieren des Symantec Management-Agent für Windows mit einer manuellen Pull-Installation 258

Ausführen einer geplanten Installation des Symantec Management-Agent für Windows 259
Anzeigen des Installationsstatusberichts 260
Anzeigen und Verwalten des Agent-Registrierungsstatus 261
Manuelle Installation von Symantec Management Agent auf UNIX-, Linux- und Mac-Computern 266
Erstellen einer CSV-Datei zum Importieren von UNIX-, Linux- und Mac-Computern 268
Installationsanforderungen für den Symantec Management Agent für UNIX, Linux und Mac 269
Angeben der Installationseinstellungen für den Symantec Management-Agent für UNIX, Linux und Mac 271
Installieren von Symantec Management-Agent für UNIX Linux und Mac mit einer manuellen Push-Installation 272
Installieren von Symantec Management-Agent unter UNIX, Linux und Mac OS mit einer manuellen Pull-Installation 276

Kapitel 16 Aktualisieren und Deinstallieren des Symantec Management Agent 278

Methoden für das Aktualisieren des Symantec Management-Agent 278
Methoden für das Deinstallieren des Symantec Management-Agent 280
Konfigurieren von Aktualisierungs- und Deinstallationsrichtlinien für den Symantec Management-Agent 280
Informationen zur Legacy-Agent-Kommunikation 284
Konfigurieren des Symantec Management-Agent-Pakets 286
Manuelles Entfernen des Symantec Management-Agent unter Windows 286

Kapitel 17 Konfigurieren des Symantec Management Agent 288

Konfigurieren des Symantec Management-Agent 288
Konfigurieren der globalen Agent-Einstellungen 290
Konfigurieren der spezifischen Einstellungen 290
Konfigurieren von Wartungsfensterrichtlinien 292

Abschnitt 5 Implementieren der Cloud-fähigen Verwaltung 296

Kapitel 18 Einführung in die Cloud-fähige Verwaltung 297

Info zu Cloud-fähiger Verwaltung 297

Kapitel 19 Vorbereiten der Umgebung auf die Cloud-fähige Verwaltung 300

Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung 300
Konfigurieren des Notification Servers für die Verwendung von HTTPS 304
Anwenden eines Zertifikats einer Stammzertifizierungsstelle auf einen verwalteten Computer 305
Umleiten eines Symantec Management-Agent für die Verwendung von HTTPS 308
Generieren und Anwenden des Site Server-Zertifikats für Zugriff des Cloud-fähigen Agent 309
Konfigurieren eines Package Servers zur Veröffentlichung von HTTPS-Paket-Codebasen 315
Konfigurieren von Sites und Site Servern zum Verarbeiten von Cloud-fähigen Agents 317

Kapitel 20 Einrichten der Cloud-fähigen Verwaltung 321

Einrichten der Cloud-fähigen Verwaltung 321
Einstellen, dass der Anwendungspool "DefaultAppPool" die Einstellung "Integriert" unter "Verwalteter Pipelinemodus" verwendet 324
Konfigurieren der Einstellungen für die Cloud-fähige Management-Agent IIS-Website 324
Info zum Vorbereiten des Internet-Gateway-Computers 327
Herunterladen und Ausführen das Internet-Gateway-Installationspakets 329
Konfigurieren des Internet-Gateway 331
Konfigurieren der Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" Richtlinie konfigurieren 334
Installieren des Symantec Management-Agent auf einem nicht verbundenen Computer 338

Kapitel 21 Ausführen von Aufgaben in der Cloud-fähigen Verwaltung 342

Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung 342
Generieren eines temporären Clientzertifikats 343
Installieren eines temporären Zertifikats auf einem verwalteten Computer 346
Widerrufen eines Zertifikats der Cloud-fähigen Verwaltung 347
Erzwingen, dass der Symantec Management-Agent ein angegebenes Gateway verwendet 350
Sichern und Wiederherstellen eines Internet-Gateways 351
Anzeigen von Berichten der Cloud-fähigen Verwaltung 353

Abschnitt 6 Verwalten von Symantec Management-Plattform-Ressourcen 354

Kapitel 22 Konfigurieren der Ressourcensicherheit 355

Konfigurieren der Ressourcensicherheit 355
Erstellen und Konfigurieren einer Organisationsansicht 358
Erstellen und auffüllen einer Organisationsansicht oder eine Gruppe 359
Erstellen und Konfigurieren von Organisationsgruppen 360
Anzeigen von Ressourcen in einer Organisationsgruppe 361
Festlegen der Sicherheit für eine Organisationsgruppe 362
Überlegungen zu Ressourcen mit Bereichsfestlegung 364

Kapitel 23 Konfigurieren der Ressourcenfilter und -ziele 369

Info zu Ressourcenfiltern 369
Erstellen oder Ändern von Filtern 370
Erstellen eines neuen Filters 372
Ändern eines vorhandenen Filters 372
Auswählen des Filterabfragetyps 373
Definieren einer Ressourcenabfrage für einen Filter 374
Definieren einer SQL-Abfrage für einen Filter 377
Ein- und Ausschließen von Elementen in/aus Filtern 378
Aktualisieren der Mitgliedschaft eines Filters 380
Durchführen von Aktionen für Filterressourcen 381
Anzeigen von Filterabhängigkeiten 382
Info zu Ressourcenzielen 383
Planen von Ressourcen-Mitgliedschaftsaktualisierungen 384

Kapitel 24 Konfigurieren von Paketen 387

Ändern der Konfigurationseinstellungen für ein Paket 387
Aktualisieren der Verteilungspunkte für ein Paket 388
Aktivieren des Zugriffs auf Pakete in einem UNC-Quellverzeichnis 389
Verwalten von Paketprogrammen 390

Kapitel 25 Verwenden von Richtlinien 392

Informationen zu Symantec Management-Plattform-Richtlinien 393
Infos zu benutzerbasierten Richtlinien 394
Verwalten von Symantec Management-Plattform-Richtlinien 395
Anwenden eine Richtlinie mit Drag and Drop 395
Festlegen der Ziele für Richtlinien oder Aufgaben 396
Ändern eines Ressourcenziels 398
Erstellen eines Ressourcenziels 399
Auswählen eines vorhandenen Ressourcenziels 400
Speichern eines benannten Ressourcenziels 400
Angeben von Filterregeln für Ressourcenziele 401
Auswählen benannter Ressourcenziele 403
Angeben von Richtlinienzeitplänen 404
Konfigurieren der Installations-, Aktualisierungs- und Deinstallationsrichtlinien für Agents und Plugins 406
Infos zu Automatisierungsrichtlinien 408
Schlüsselkomponenten von Automatisierungsrichtlinien 409
Verwalten von Automatisierungsrichtlinien 410
Erstellen und Ändern von geplanten Automatisierungsrichtlinien 414
Erstellen und Ändern von meldungsbasierten Automatisierungsrichtlinien 416
Angeben der Datenquelle für Automatisierungsrichtlinien 419
Festlegen der Aktion für Automatisierungsrichtlinien 421
Auswählen von Aufträgen oder Aufgaben für die Automatisierungsrichtlinie 423
Erstellen und Ändern von Automatisierungsrichtlinien-Aufgaben 423

Kapitel 26 Verwenden von Aufgaben und Aufträgen 426

Informationen zu Task Management 426
Task Management-Komponenten 428
Wie Task Server die Tickle-Funktion verwendet 429
Verwendung von Aufgaben, Jobs und Richtlinien 432
Informationen zu ausgeführten Aufgaben in der Hierarchie 433
Sequenzieren von Aufgaben 436

Bereitstellen eines Task Server 437
Erstellen einer Aufgabe 438
Erstellen eines Jobs 439
Ausführen eines Auftrags oder einer Aufgabe mit Drag & Drop 441
Ausführen eines Jobs oder einer Aufgabe 442
Erneutes Ausführen einer fehlgeschlagenen Aufgabe 442
Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag 444
Anzeigen des Aufgabenstatus auf dem Symantec Management-Agent 445
Anzeigen und Bearbeiten von Berechtigungen für einen Aufgabentyp 445
Erstellen von Aufgaben für die Eingabe oder Ausgabe von Aufgabeneigenschaften 446
Bereinigen von Aufgabendaten 449
Bereinigen von Aufgabenversionsdaten 450
Ändern der Client Task Agent-Einstellungen 451
Zugriff auf das Job- und Aufgabenportal 452

Kapitel 27 Verwenden des Ressourcenmanagers 454

Informationen zur Ressourcenverwaltung 454
Zugreifen auf Ressourcenmanager 455
Anzeigen der Inventardaten für eine Datenklasse 456
Anzeigen der Ereignisdaten für eine Datenklasse 456
Hinzufügen einer Ressource zu einer Organisationsgruppe 457
Ressourcenmanager-Aufgaben 457

Kapitel 28 Verwenden von Notification Server-Berichten 460

Infos zu Notification Server-Berichten 460
Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten 461
Extrahieren von Notification Server-Berichtsergebnissen 462
Anzeigen von Notification Server-Berichtsergebnissen 464
Verwenden der Notification Server-Berichtsergebnisse 465
Speichern von Notification Server-Berichtsergebnissen als Datei 466
Erstellen eines statischen Filters aus Notification Server-Berichtergebnissen 467
Speichern von Notification Server-Berichtsergebnissen als Snapshot 468

Speichern von Notification Server-Berichtsergebnissen als Web-Part 469

Kapitel 29 Erstellen benutzerdefinierter Notification Server-Berichte 471

Komponenten eines benutzerdefinierten Notification Server-Berichts 471
Erstellen und Ändern benutzerdefinierter Notification Server-Berichte 473
Erstellen eines benutzerdefinierten Notification Server-Berichts 476
Ändern eines vorhandenen benutzerdefinierten Notification Server-Berichts 478
Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht 478
Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht 480
Definieren von Parametern und Value Providers für einen benutzerdefinierten Bericht 481
Erstellen oder Ändern einer Diagrammansicht für einen benutzerdefinierten Bericht 483
Erstellen oder Ändern einer Rasteransicht für einen benutzerdefinierten Bericht 485
Einrichten der Drilldown-Aktionen für einen benutzerdefinierten Bericht 486
Festlegen der erweiterten Eigenschaften eines benutzerdefinierten Berichts 489

Kapitel 30 Anzeigen von Ressourceninformationen 491

Informationen zu Ressourcen 491
Anzeigen von Ressourcendatenklasseinformationen 492
Anzeigen von Ressourcenzuordnungstypinformationen 492
Anzeigen von Ressourcentypinformationen 492

Abschnitt 7 Verwalten von CMDB-Daten mit Data Connector 494

Kapitel 31 Einführung in Data Connector 495

Infos zu Data Connector 495
Funktionsweise von Data Connector 495

Einsatzmöglichkeiten von Data Connector 497

Kapitel 32 Ausführen von Datenverwaltungsaufgaben 498

Importieren und Exportieren von Daten 498
Infos zum Vorbereiten von Daten vor dem Importieren 500
Erstellen einer Datenquellendefinition 500
Erstellen einer Datenübertragungsregel 501
Erstellen eines Ressourcen-Suchschlüssels 502
Ausführen einer Datenübertragungsregel als Aufgabe 503
Anzeigen von Datenübertragungsübersichten 504
Prüfen der Funktionsweise von Datenübertragungsregeln 504
Erstellen einer CMDB-Regel zum Bearbeiten von CMDB-Daten 505
Ausführen einer CMDB-Regel als Aufgabe 506
Erstellen einer virtuellen Datenklasse 507
Konfigurieren von Bereinigungsoptionen für die ausführliche Protokollierung in Data Connector 508

Anhang A Sicherheitsrechte und -berechtigungen 509

Sicherheitsprivilegkategorien 510
Kategorien von Sicherheitsberechtigungen 512
Verbindungsprofil-Privilegien 513
Verwaltungsrechte 514
Systemrechte 516
Identifikationsdatenprivilegien 518
Workflow-Verzeichnisprivilegien 519
Symantec Management Console-Rechte 519
Software Management-Rechte 521
Kontextmenü-Privilegien 522
Kontextmenü: Privilegien für Connector-Beispiele 524
Kontextmenü: Hierarchie-Privilegien 524
Kontextmenü - Privilegien "Aktionen" 525
Kontextmenü: Privilegien zum Einstellen des Asset-Status 527
Ressourcenverwaltungsberechtigungen 527
Systemberechtigungen 528
Task Server-Berechtigungen 528
Berichtsberechtigungen 529
Richtlinienberechtigungen 529
Ordnerberechtigungen 529
Filterberechtigungen 530
Verbindungsprofil-Berechtigungen 530
Credential Manager-Berechtigungen 531

Anhang B Symantec Management Agent 532

Empfohlene Datenaktualisierungsintervalle für den Symantec Management-Agent 532
Problemlösungsbefehle für Symantec Management-Agent für UNIX, Linux und Mac 533

Anhang C Cloud-fähige Verwaltung - Referenzthemen 538

Kommandozeilenprogramme des Notification Servers 538
Unterstützte Konfigurationen für Package Server in einer gemischten Umgebung 539
Auswirkungen der Cloud-fähigen Verwaltung auf die Funktionen der Site Server 540
Internet-Gateway-Verwaltungsskripts 542
Info zur Internet-Gateway-Lastverteilung 543
Parameter für Installationspakete Cloud-fähiger Agents 544
Kommandozeilen-Switches für Cloud-fähige Agents 545

Anhang D Benutzerdefinierten Berichtseinstellungen 548

Seite "Benutzerdefinierte Berichte bearbeiten" 549
Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle" 550
Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrage" 553
Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Felder" 557
Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Parametrisierte Abfrage" 558
Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageparameter" 559
Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Filterausdrücke" 560
Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Daten-Snapshots" 560
Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageauflösung" 563
Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Ergebnisse" 564
Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Ansichten" für eine Diagrammansicht 565
Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Ansichten" für eine Rasteransicht 568

Quellfelder bearbeiten Dialogfeld 570
"Parameter wird bearbeitet" Dialogfeld 571

Anhang E Skriptfähige Felder zum Ändern der Import-/Export- und CMDB-Regeln für Ressourcen 573

Skriptfähige Felder zum Ändern der Import-/Exportregel für Ressourcen und CMDB-Regel 573
Ausdruckssyntax 574
Ausdrucksoperatoren 575
Benutzerdefinierte Werte 575
Zeichenfolgenoperatoren 575
Platzhalterzeichen 576
Aggregationstypen 576
Ausdrucksfunktionen 576

Anhang F Symantec™ Management-Plattform 7.5 - Rechtliche Hinweise zu Drittanbietern 580

Rechtliche Hinweise zu Drittanbietern 581
7-Zip 581
Apache HTTP Server 582
Apache Xerces C++ 585
Boost 589
Bouncy Castle 590
Curl 591
glibc 591
Libatomics_Ops 601
LibXML2 602
Makeself 603
Microsoft Anti-Cross Site Scripting Library 609
OpenPegasus 610
OpenSSL 0.9.8u 611
OpenSSL 0.9.8y 614
OpenSSL 1.0.1e 617
plists-cs 620
SQLite 620
Windows Template Library 'WTL' v8.0 621
Zlib 622

Index 623

Abschnitt 1

Einführung in die Schlüsselkomponenten von IT Management Suite

- Kapitel 1. Einführung in Symantec Management-Plattform
- Kapitel 2. Einführung in die Symantec Management Console

Kapitel 1

Einführung in Symantec Management-Plattform

In diesem Kapitel werden folgende Themen behandelt:

- Info zur Symantec Management-Plattform
- Neue Funktionen in IT Management Suite 7.5
- Komponenten der Symantec Management-Plattform
- Funktionsweise von pcAnywhere Solution
- Infos zum Hinzufügen von Produkten zur Plattform
- Weitere Informationen

Info zur Symantec Management-Plattform

Symantec Management-Plattform bietet Dienste, die von IT-bezogenen Lösungen genutzt werden. Lösungen werden in die Plattform integriert, sodass sie die Dienste der Plattform, wie z. B. Sicherheit, Berichterstattung, Kommunikation, Paketverteilung und Configuration Management Database (CMDB)-Daten nutzen können. Da Lösungen die gleiche Plattform verwenden, können sie sowohl Plattformdienste als auch Daten gemeinsam nutzen. Gemeinsam genutzte Daten sind in der Regel nützlicher als lösungsspezifische. Beispiel: Eine Lösung sammelt Daten über die Software, die auf Unternehmenscomputern installiert ist und eine andere Lösung nutzt die Daten, um Softwarelizenzen zu verwalten. Und eine dritte Lösung kann dieselben Daten zur Softwareaktualisierung verwenden. Diese enge Integration von Lösungen und Plattform erleichtert die Verwendung der verschiedenen Lösungen, da sie alle in einer gemeinsamen Umgebung und über eine gemeinsame Benutzerschnittstelle verwaltet werden.

Die Plattform stellt die folgenden Dienste zur Verfügung:

- Rollenbasierte Sicherheit
- Clientkommunikation und -verwaltung
- Ausführen von geplanten oder von Ereignissen ausgelösten Aufgaben und Richtlinien
- Verteilen und Installieren von Paketen
- Berichterstellung
- Zentralisierte Verwaltung über eine einzelne, gemeinsame Benutzerschnittstelle
- Configuration Management Database (CMDB)
- Software Management Framework

Wenn Sie eine Lösung oder Suite installieren, wird auch die Plattform installiert, wenn dies nicht bereits geschehen ist.

Siehe "Komponenten der Symantec Management-Plattform" auf Seite 27.

Siehe "Funktionsweise von pcAnywhere Solution" auf Seite 28.

Siehe "Infos zum Hinzufügen von Produkten zur Plattform" auf Seite 29.

Siehe "Neue Funktionen in IT Management Suite 7.5" auf Seite 24.

Neue Funktionen in IT Management Suite 7.5

In Version 7.5 von IT Management Suite werden die folgenden neuen Funktionen eingeführt:

Tabelle 1-1 Liste der neuen Funktionen

Funktion	Beschreibung
Allgemeine Verbesserungen	■ Administratoren werden eine Steigerung der Konsolenleistung von bis zu Faktor 15 erkennen. ■ Die neue Funktion "Aufgabe erneut ausführen" ist auf Computern verfügbar, auf denen die Aufgabe fehlschlug. ■ Mit dem neuen Software Delivery-Flipbook können Sie Übersichtsinformationen zu Schnellverteilungsaufgaben und verwaltete Verteilungsrichtlinien in Ihrer Umgebung anzeigen und darauf reagieren.

Funktion	Beschreibung
Cloud-fähige Verwaltung (CEM)	Mit der Cloud-fähigen Verwaltung können Sie Endgeräten verwalten, selbst wenn diese Endgeräte nicht mit dem Unternehmensnetzwerk über VPN verbunden sind. Diese Funktion hilft beim Verbessern der Software- und Patch-Bereitstellungsabdeckung Ihrer mobilen und Tele-Angestellten. CEM ermöglicht eine vollständig sichere Kommunikation zwischen Roaming-Endgeräten und Notification Servers im internen Netzwerk. Die folgenden Lösungen und Funktionen werden über CEM unterstützt: ■ Task Management Mit Task Management können Sie beliebige Aufgabentypen im CEM-Modus ausführen. Die Tickle-Verbindung zum Task Server wird jedoch nicht in CEM-Modus hergestellt und die unmittelbare Aufgabenausführung ist nicht verfügbar. Die Aufgaben können entsprechend den Standardeinstellungen mit einer Verzögerung von bis zu 60 Minuten ausgeführt werden. Das Ausführen eines Task Server auf einem Cloud-fähigen, über das Internet-verwalteten Clientcomputer wird nicht unterstützt und kann zu unerwünschtem Verhalten führen. ■ Inventory Solution Hardware-, Software-, benutzerdefinierte , Serverinventarisierungs- und Application Metering-Funktionen werden unterstützt CEM wird nur unter Windows unterstützt. ■ Software Management Solution ■ Patch Management Solution
Agent-Registrierung	Zusammen mit der Cloud-fähigen Verwaltung, mit der Sie Geräte verwalten können, die außerhalb der Firewall sind, wurde die eine Funktion zum Registrieren von Agent in IT Management Suite 7.5 hinzugefügt, um sicherzustellen, dass nur vertrauenswürdige Endgeräte mit Notification Server kommunizieren können. Die Agent-Registrierung erfordert ein Endgerät, das mit Notification Server kommunizieren kann, bevor es von diesem Notification Server verwaltet werden kann.
Modus "Legacy-Agent-Kommunikation" (LAC)	Mit dem Modus "Legacy-Agent-Kommunikation" können Sie steuern, ob die Computer, die ältere Versionen von Symantec Management Agent verwenden, mit dem auf Version 7.5 aktualisierten Notification Server kommunizieren können. Mit dieser Option können Sie die Agents in Ihrer Umgebung in Phasen aktualisieren, und nicht alle auf einmal gleich nach dem Aktualisieren von Notification Server.

Funktion	Beschreibung
Die Liste der unterstützten Betriebssystemen wurde erweitert.	Das folgende Betriebssystem wird jetzt für die Installation der Symantec Management-Plattform und ihrer Komponenten unterstützt: ■ Windows Server 2008 R1 SP2 (64-Bit) Die folgenden Versionen von SQL Server werden jetzt für die Configuration Management Database (CMDB) unterstützt: ■ Microsoft SQL Server 2008 R2 SP1 ■ Microsoft SQL Server 2008 SP3 ■ Microsoft SQL Server 2012 Die folgenden Betriebssysteme werden jetzt für die Installation des Symantec Management Agent unterstützt: ■ Windows 7 SP1 ■ Windows 8 ■ Windows Server 2008 R1 SP2 ■ Windows Server 2012 ■ Red Hat Enterprise Linux 5.7, 5.8, 6.2 und 6.3 **Hinweis:** Windows 8 und Windows Server 2012 werden nicht für den Einsatz als Site Server unterstützt.
Unterstützung für Internet Explorer 10 (Kompatibilitätsmodus) im Softwareportal	Das Softwareportal von Software Management Solution unterstützt jetzt Internet Explorer 10 im Kompatibilitätsmodus.
Die neue Protokollanzeige wurde implementiert.	Die folgenden neuen Funktionen sind in der neuen Protokollanzeige enthalten: ■ Sie können sehr viele Protokolldateien laden, ohne viele der Serverressourcen zu verbrauchen. ■ Der Filtermechanismus wurde vereinfacht und die Filterdefinitionen können zur späteren Verwendung gespeichert werden. ■ Es gibt jetzt eine Lesezeichenfunktion. ■ Sie können eine Suche in den Protokolldateien durchführen, ohne die Protokolldateien in die Protokollanzeige zu laden.
Die Funktion "SuppressReportAutorun" wurde implementiert.	Ist "SuppressReportAutorun" aktiviert und Sie öffnen einen beliebigen Bericht, wird der Bericht nicht sofort ausgeführt. Damit die Ergebnisse des Berichts angezeigt werden, müssen Sie auf "Aktualisieren" klicken. Standardmäßig ist die Funktion "SuppressReportAutorun" deaktiviert. Sie können sie in "NS-Konfigurator" unter "Core-Einstellungen > Benutzeroberfläche > Bericht > SuppressReportAutorun" aktivieren.

Funktion	Beschreibung
Die CMDB Solution-Lizenzprüfung wurde entfernt.	Die Lizenzprüfung für CMDB Solution wurde entfernt. Die Lösung ist daher in allen Altiris-Lösungen als Funktion verfügbar. Sie können jetzt CMDB Solution als Funktion der Inventarisierung, Client Management Suite und Server Management Suite installieren. Sie wird bereits mit Asset Management Suite, ServiceDesk und IT Management Suite installiert. **Hinweis:** In einer Hierarchie muss CMDB Solution auf dem übergeordneter Notification Server installiert werden. Installieren Sie CMDB Solution nicht auf einem untergeordneter Notification Server.
Die Komponente "Out of Band Management" wurde entfernt.	In Version 7.5 von IT Management Suites ist die Komponente "Out of Band Management" nicht mehr verfügbar. Wenn Sie von früheren Versionen von IT Management Suite aktualisieren, entfernt das Dienstprogramm "OOBRemover" die Out of Band Management-Elemente aus Notification Server, Site Server und Clientcomputern.
Änderungen in Versionshinweisen zu IT Management Suite 7.5 und der Dokumentation zu Symantec Management-Plattform 7.5.	In IT Management Suites 7.5 gelten die meisten lösungsspezifischen Versionshinweise für die Lösungen, die Komponenten der folgenden Suites sind nicht mehr: ■ Asset Management Suite ■ Client Management Suite ■ Server Management Suite Sie finden die Informationen aus den veralteten lösungsspezifischen Versionshinweisen in den Versionshinweisen zurr jeweiligen Suite. Weitere Informationen finden Sie im folgenden Artikel: http://www.symantec.com/docs/DOC5702

Komponenten der Symantec Management-Plattform

Tabelle 1-2 Komponenten der Symantec Management-Plattform

Komponente	Beschreibung
Notification Server und Symantec Management Console	Dieser Symantec Management-Plattform-Dienst verarbeitet Ereignisse, stellt die Kommunikation mit verwalteten Computern her und koordiniert die Funktionen der anderen Symantec Management-Plattform-Dienste. Die Konsole ist die webbasierte Benutzeroberfläche des Notification Server-Computers, mit der Sie die Plattform und ihre Lösungen verwalten können. Siehe "Informationen zum Notification Server" auf Seite 66. Siehe "Info zur Symantec Management Console" auf Seite 33.

Komponente	Beschreibung
Configuration Management Database (CMDB)	Die Datenbank, in der alle Informationen über verwaltete Computer gespeichert sind. Siehe "Konfigurieren von Configuration Management Database" auf Seite 78.
Site Server	Symantec Management-Plattform kann einige Typen von Middleware-Komponenten hosten, z. B. Paketdienste, Aufgabedienste und Deployment Site-Dienste. Der offizielle Name für eine Middleware-Komponente ist "Site Service". Komponenten, die als Host für einen Site Service fungieren, werden als "Site Server" bezeichnet. Site Server können eine oder mehrere dieser Dienste hosten. Siehe "Info zu Site Services" auf Seite 133.
Symantec Management-Agent	Die Software, die auf einem Computer installiert wird, damit er von Notification Server überwacht und verwaltet werden kann. Nachdem der Symantec Management-Agent installiert ist, ist dieser Computer ein verwalteter Computer. Siehe "Infos zu Symantec Management-Agent" auf Seite 246.
Software Management Framework	Eine Schnittstelle, mit der Sie Software-Ressourcen aus dem Softwarekatalog erstellen und verwalten können. Außerdem können Sie damit die Pakete in der Softwarebibliothek verwalten. Die Anzeige "Software" stellt einen zentralen Ort zum Initiieren der softwarebezogenen Aufgaben bereit, die in Ihrem Unternehmen durchgeführt werden.
Berichte	Ein Verfahren zum automatisierten Sammeln von Informationen. Sie können Berichte für verwaltete Computer von der Symantec Management Console aus anzeigen. Siehe "Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten" auf Seite 461.

Siehe "Info zur Symantec Management-Plattform" auf Seite 23.

Siehe "Funktionsweise von pcAnywhere Solution" auf Seite 28.

Funktionsweise von pcAnywhere Solution

Symantec pcAnywhere Solution verwendet die Fernsteuerungstechnologie Sie können eine Verbindung zu einem anderen Computer oder Server herstellen und so arbeiten, als säßen Sie direkt vor dem Computer. pcAnywhere Solution unterstützt Netzwerkverbindungen über LAN, WAN oder das Internet.

Grundlegende Kenntnisse der pcAnywhere-Terminologie sind von Vorteil. So wird der Clientcomputer beispielsweise als Hostcomputer bezeichnet, da er den Host für die Verbindung darstellt. Der Computer des Administrators wird Remote-Computer oder Konsole genannt. Diese Terminologie stammt aus dem Bereich des Mainframe-Computing, bei dem Remote-Benutzer üblicherweise mit

einem Server oder einem Großrechner verbunden sind. In pcAnywhere wird der sitzungsinterne Frame als Anzeige bezeichnet.

In den meisten Fällen wird die Verbindung durch einen Remote-Benutzer initiiert. Dieser gibt die für die Verbindung mit dem Hostcomputer erforderlichen Informationen an. Der Remote-Benutzer kann auch Optionen zum Erhöhen der Sicherheit oder zum Optimieren der Leistung festlegen. Zum Herstellen einer Verbindung muss der Hostcomputer so eingerichtet sein, dass er auf eingehende pcAnywhere Solution-Verbindungen wartet.

pcAnywhere Solution enthält die pcAnywhere-Web-Parts für die Konfiguration, Notification Server-Berichte, die Benutzeroberfläche "pcAnywhere Manager" und die Software "pcAnywhere Solution".

pcAnywhere Solution bietet die folgenden Funktionen:

- Rollenbasierte Sicherheit durch Console-Seiten
- Einstellungen für die Steuerung des verwalteten Hosts
- Überwachungsprotokolle und Berichterstellung
- Unterstützung für Sicherheits- und Bereichsfestlegungsmechanismen
- Integration von VNC und RDP

pcAnywhere Solution enthält außerdem folgende Funktionen von Notification Server:

- Task Server
- Hierarchie
- Benutzerbasierte Richtlinien

Siehe "Info zur Notification Server-Hierarchie" auf Seite 160.

Siehe "Informationen zu Task Management " auf Seite 426.

Siehe "Infos zu benutzerbasierten Richtlinien" auf Seite 394.

Infos zum Hinzufügen von Produkten zur Plattform

Eine Vielzahl von Produkten kann auf der Symantec Management-Plattform ausgeführt werden. Symantec und andere Unternehmen liefern zusätzliche Produkte, die auf der Plattform laufen. Beispielsweise hilft die Symantec Client Management Suite beim Verwalten von Endpunktcomputern und die Symantec Server Management Suite beim Verwalten von Servern.

Mit dem Symantec Installation Manager können Sie die Installation von zusätzlichen Produkten auf der Plattform verwalten. Auf der Seite "Neue Produkte installieren" von Symantec Installation Manager können Sie eine Liste von verfügbaren Produkten anzeigen. Sie können dann einfach ein Produkt installieren und evaluieren. Für die

meisten Produkte wird eine 30-tägige Testlizenz angeboten. Sie können eine Liste aller installierten Produkte auf der Seite "Installierte Produkte" von Symantec Installation Manager anzeigen.

Wenn Sie Produkte erwerben, verwaltet Symantec Installation Manager auch die Lizenzen. Auf der Seite "Produktlizenzierung" können Sie Lizenzen auf installierte Produkte anwenden und den Status von angewendeten Lizenzen anzeigen.

Weitere Informationen finden Sie im *Implementierungs- und Planungshandbuch für IT Management Suite*.

Weitere Informationen

Machen Sie sich anhand der folgenden Dokumentationsressourcen mit der Verwendung des Produkts vertraut.

Tabelle 1-3 Dokumentationsressourcen

Dokument	Beschreibung	Speicherort
Versionshinweise	Informationen über neue Funktionen und wichtige Themen.	Die Seite "Unterstützte Produkte A-Z" ist unter folgender URL verfügbar: http://www.symantec.com/business/support/index?page=products Öffnen Sie die Supportseite Ihres Produkts und klicken Sie dann unter "Häufige Themen" auf "Versionshinweise".
Benutzerhandbuch	Informationen zur Verwendung dieses Produkts, einschließlich detaillierter technischer Informationen und Anweisungen zur Ausführung von Routineaufgaben.	■ Die Dokumentationsbibliothek ist in der "Symantec Management Console" im Menü Hilfe verfügbar. ■ Die Seite "Unterstützte Produkte von A-Z" ist unter folgender URL verfügbar: http://www.symantec.com/business/support/index?page=products Öffnen Sie die Supportseite Ihres Produkts und klicken Sie dann unter "Allgemeine Themen" auf "Dokumentation".

Dokument	Beschreibung	Speicherort
Hilfe	Informationen zur Verwendung dieses Produkts, einschließlich detaillierter technischer Informationen und Anweisungen zur Ausführung von Routineaufgaben. Hilfe ist für "Solution" und "Suite" verfügbar. Diese Informationen sind im Format "HTML-Hilfe" verfügbar.	Die Dokumentationsbibliothek ist in der "Symantec Management Console" im Menü Hilfe verfügbar. Kontextbezogene Hilfe ist für die meisten Dialogfelder der Symantec Management Console verfügbar. Es gibt folgende Möglichkeiten zum Öffnen der kontextbezogenen Hilfe: ■ Klicken Sie auf die Seite und drücken Sie dann die Taste "F1". ■ Der Befehl "Kontext" ist in der Symantec Management Console im Menü "Hilfe" verfügbar.

Zusätzlich zur Produktdokumentation können Sie die folgenden Ressourcen nutzen, um sich mit Symantec-Produkten vertraut zu machen.

Tabelle 1-4 Symantec-Produkt-Informationsressourcen

Ressource	Beschreibung	Speicherort
SymWISE-Support datenbank	Artikel zu Symantec-Produkten sowie Vorfälle und Probleme im Zusammenhang mit Symantec-Produkten.	http://www.symantec.com/business/theme.jsp?themeid=support-knowledgebase

Ressource	Beschreibung	Speicherort
Symantec Connect	Eine Online-Ressource, die Foren, Artikel, Blogs, Downloads, Ereignisse, Videos, Gruppen und Ideen für Benutzer von Symantec-Produkten enthält.	http://www.symantec.com/connect/endpoint-management/forums/endpoint-management-documentation Hier finden Sie die Liste von Links zu den verschiedenen Gruppen auf Connect: ■ Bereitstellung und Imaging http://www.symantec.com/connect/groups/deployment-and-imaging ■ Erkennung und Inventarisierung http://www.symantec.com/connect/groups/discovery-and-inventory ■ ITMS-Administrator http://www.symantec.com/connect/groups/itms-administrator ■ Mac-Verwaltung http://www.symantec.com/connect/groups/mac-management ■ Monitor Solution und Serverzustand http://www.symantec.com/connect/groups/monitor-solution-and-server-health ■ Patch-Management http://www.symantec.com/connect/groups/patch-management ■ Berichte http://www.symantec.com/connect/groups/reporting ■ ServiceDesk und Workflow http://www.symantec.com/connect/workflow-servicedesk ■ Softwareverwaltung http://www.symantec.com/connect/groups/software-management ■ Serververwaltung http://www.symantec.com/connect/groups/server-management ■ Workspace-Virtualisierung und Streaming http://www.symantec.com/connect/groups/workspace-virtualization-and-streaming

Kapitel 2

Einführung in die Symantec Management Console

In diesem Kapitel werden folgende Themen behandelt:

- Info zur Symantec Management Console
- Info zu Konsolenansichten
- Aufrufen der Symantec Management Console
- Aufrufen der Dokumentation in der Symantec Management Console
- Aufrufen der Seite "Mein Portal"
- Zugreifen auf die Startseite von Notification Server Management
- Anpassen der Symantec Management Console

Info zur Symantec Management Console

Symantec Management Console (normalerweise als "die Konsole" bezeichnet) ist eine webbasierte Benutzeroberfläche, die das primäre Tool für die Kommunikation mit Notification Server und seinen Komponenten und für das Verwalten von Ressourcen ist.

Symantec Management Console ist in die folgenden Bereiche unterteilt:

Header	Der obere Teil der Konsole, der Folgendes enthält: ■ Menüs, über die Sie auf Seiten und Dialogfelder der Konsole zugreifen können, die die Verwaltungsfunktionen für Notification Server zur Verfügung stellen. Symantec-Lösungen, die auf dem System installiert werden, fügen unter Umständen dem Menü neue Objekte hinzu. ■ Suchfeld, über das Sie die Ressourcendaten nach den gewünschten Ressourcen durchsuchen können. Geben Sie hier den Suchbegriff ein. ■ Eine Mini-Leiste, die den Menüpfad zur derzeit angezeigten Seite anzeigt.
Inhaltsbereich	Der Teil der Konsole, die sich unter dem Header befindet, kann Folgendes anzeigen: ■ Ansicht Eine Ansicht besteht aus einem Strukturansichts- und einem Inhaltsteilfenster. Die Strukturansicht im linken Teilfenster zeigt eine hierarchische Anordnung von Objekten an, die Sie auswählen und mit denen Sie arbeiten können. Das Inhaltsteilfenster im rechten Teilfenster zeigt Seiten je nach der Strukturansichtauswahl an. ■ Portalseite Eine Portalseite zeigt eine Sammlung unterschiedlicher Informationen in Web-Parts an. Notification Server enthält vordefinierte Portalseiten und andere Portalseiten sind möglicherweise mit Lösungen enthalten. Sie können auch eigene Portalseiten erstellen. ■ Ganze Seite Eine ganze Seite umfasst ein einzelnes Inhaltsfenster ohne die Baumstruktur.

Einige Seiten der Konsole unterstützen Personalisierung, also die Fähigkeit einer Konsolenseite, den Zustand seiner Steuerelemente je nach Benutzer beizubehalten. Beispielsweise kann Benutzer A an einem Tag eine Filterseite öffnen und die Spalten im Raster neu anordnen, um ihrer persönlichen Präferenz zu entsprechen. Unterdessen öffnet Benutzer B die gleiche Seite, aber lässt das Raster in seiner Standardkonfiguration. Wenn die Benutzer am folgenden Tag diese Filterseite öffnen, wird Benutzer A die Seite angezeigt, wie sie am Tag zuvor konfiguriert wurde. Benutzer B wird weiterhin die Standardansicht vom Tag zuvor angezeigt.

Die Personalisierung wird derzeit auf die Berichterstellungs- und Filterseiten sowie auf den Zustand der Verzeichnisstruktur in den Ansicht-Seiten angewendet. Darüber hinaus wird die Seite "Mein Portal" für jeden Benutzer angepasst.

Info zu Konsolenansichten

Eine Ansicht ist ein Layout mit zwei Teilfenstern mit einer Verzeichnisstruktur im linken Teilfenster und Inhalt im rechten Teilfenster. Die Verzeichnisstruktur enthält Links zu Symantec Management Console-Elementen und ermöglicht es Ihnen, Elemente aus verschiedenen Teilen der Konsole in einer geeigneten Struktur anzuordnen. Ein Element kann mehrmals in einer Ansicht und beliebig oft in verschiedenen Ansichten angezeigt werden. Eine Ansicht kann Ordner, Elementverknüpfungen und Weblinks enthalten. Die Symantec Management-Plattform und -Lösungen enthalten vordefinierte Ansichten, die Sie bei Bedarf ändern und erweitern können. Sie können auch eigene Ansichten erstellen.

Siehe "Erstellen und Ändern von Ansichten" auf Seite 57.

Siehe "Hinzufügen neuer Elemente direkt zu einer Ansicht" auf Seite 58.

Über Ansichten können Sie die Symantec Management-Plattform- und Lösungsfunktionalität organisieren und aufrufen. Es empfiehlt sich, Ansichten entsprechend einzurichten, um die Funktionalität darzustellen, die von einer Lösung bzw. Funktion zur Verfügung gestellt wird, oder um Benutzer in einer bestimmten Rolle Zugriff auf die entsprechenden Aufgaben zu ermöglichen.

Die Standard-Verzeichnisstruktur, die Ihnen im linken Teilfenster angezeigt wird, ist die reale Ordnerstruktur. Jedes Element wird in der realen Struktur nur einmal angezeigt. Bei Ordnern in einer Ansicht kann es sich um virtuelle Ordner handeln, die in der realen Struktur nicht existieren, oder es können Links zu realen Ordnern sein. Ein Link zu einem realen Ordner enthält alles unter diesem Ordner. Wenn neue Objekte zur realen Struktur in diesem Ordner hinzugefügt werden, sind sie automatisch in der Ansicht enthalten. Sie können Elemente in einem Ordner nicht von einer Ansicht ausschließen, aber Sie können sie aus der Ansicht löschen. Dadurch wird die Verknüpfung zwischen der Ansicht und dem Element aufgehoben: Das reale Element wird jedoch nicht gelöscht.

Die Sicherheit wirkt sich auf Ansichten aus. Somit hängt alles, was Sie in einer Ansicht sehen, von Ihren Sicherheitsprivilegien und -berechtigungen ab. Um ein Privileg oder eine Berechtigung auf einen Ordner in einer Ansicht zu haben, muss sie direkt in der Ansicht und auch im realen Ordner festgelegt werden. Sie sehen unter Umständen nur einige der Elemente in einer Ansicht, aber andere Benutzer können mehr oder weniger sehen.

Info zur Ansicht "Computer"

Hinweis: Eins der folgenden Produkte muss installiert sein, damit diese Seite angezeigt wird: Deployment Solution (eigenständiges Produkt), IT Management Suite, Server Management Suite oder Client Management Suite.

Um auf die erweiterte Ansicht Computer zuzugreifen, klicken Sie in der Symantec Management Console auf "Verwaltung > Computer".

Die Ansicht "Computer" bietet zwei Möglichkeiten, Computern in Ihrer Umgebung zu betrachten: über die Einzelansicht und über die Übersicht.

Hinweis: Sie können zwischen diesen Ansichten wechseln, indem Sie auf die doppelten Pfeile (>> oder <<) auf der rechten Seite der Überschrift "Computer" klicken.

Einzelansicht

Die Einzelansicht gibt Ihnen Details über einen bestimmten Computer. Sie können diesen Computer links im Navigationsbereich oder im Dialogfeld der Suche im Bereich "Liste" angeben.

Tabelle 2-1 Einzelansicht

Navigationsbereich **(enthält gespeicherte Suchvorgänge, Organisationsansichten und Gruppen)**	**Listenbereich** **(zeigt den/die Computer aus der ausgewählten gespeicherten Suche, der Organisationsansicht oder der Gruppe an)**	**Detailseite** **(zeigt Bestandsdetails über den/die ausgewählten Computer an)**
Computer Gespeicherte Suchvorgänge ■ Neue Computer ■ Installierter Agent ■ <Benutzerdefiniert> Alle Computeransichten ■ Alle Computer ■ Virtueller Computer Blades: ■ Computer ■ Aufträge/Aufgaben ■ Richtlinien ■ Software	Suchfeld Suchergebnisse	Flipbook-Seiten: ■ Allgemein ■ Identifizierung ■ Symantec Management Agent-Details (Agent muss installiert sein) ■ Hardware ■ Netzwerk ■ Laufwerke ■ Speichermodule ■ Microsoft Hotfixes ■ Lizenzierte Programme Blades ■ Aufträge/Aufgaben ■ Richtlinien ■ Software

Übersicht

In der Übersicht ist zusätzlich ein Flipbook mit drei Seiten enthalten, das Informationen zu Softwareverteilungen, Herstellern und Betriebssystemen in Ihrer Umgebung liefert, bei denen Handlungsbedarf besteht. Die Auswahl im Navigationsbereich beeinflusst die Ergebnisse im Übersichtsbereich und im Listenbereich. Durch Klicken auf eine Grafik oder ein Legendenelement in den Seiten des Flipbook wird das Ergebnis weiter verfeinert. Dann können Sie in der erweiterten Suche mehr Suchkriterien hinzufügen.

Sie können zwischen Flipbook-Seiten wechseln, indem Sie auf die Links in den Flipbook-Seiten klicken.

Tabelle 2-2 Übersicht

Navigationsbereich **(enthält gespeicherte Suchvorgänge, Organisationsansichten und Gruppen)**	**Übersichtsbereich** **(Enthält ein Flipbook mit 3 Seiten)**	**Listenbereich** **(zeigt den/die Computer aus der ausgewählten gespeicherten Suche, der Organisationsansicht oder der Gruppe an)**
Computer	■ Softwareverteilungen ■ Hersteller ■ Betriebssysteme	Suchfeld
Gespeicherte Suchvorgänge ■ Neue Computer ■ Installierter Agent ■ <Benutzerdefiniert>		Suchergebnisse
Alle Computeransichten ■ Alle Computer ■ Virtueller Computer		
Blades ■ Computer ■ Aufträge/Aufgaben ■ Richtlinien ■ Software		

Mit der Ansicht "Computer" können Sie folgende Aufgaben durchführen:

- Suchen nach Computern und Speichern der Suchergebnisse, um diese als benutzerdefinierter Filter für Zielcomputer mit Aufträgen, Aufgaben, Richtlinien oder Softwareverteilungen wiederzuverwenden.
  Siehe "Suchen nach einem Computer und Speichern der Suche als Filter" auf Seite 39.
- Erstellen und Verwalten von Organisationsansichten und Gruppen.
  Siehe "Erstellen und auffüllen einer Organisationsansicht oder eine Gruppe" auf Seite 359.
- Verschieben von Computern per Drag & Drop in Organisationsansichten und Gruppen.
  Siehe "Erstellen und auffüllen einer Organisationsansicht oder eine Gruppe" auf Seite 359.

- Anzeigen von Übersichtsinformationen für Schnellverteilungsaufgaben und Richtlinien für kontrollierte Verteilung und entsprechende Reaktion darauf.
  Siehe "Erneutes Ausführen einer fehlgeschlagenen Aufgabe" auf Seite 442.
- Anzeigen von Übersichtsinformationen für Hardware-Hersteller und Betriebssysteme.

Suchen nach einem Computer und Speichern der Suche als Filter

In der Ansicht "Computer" können Sie nach einem bestimmten Computer oder einer Gruppe Computern suchen, indem Sie eine vordefinierte gespeicherte Suche anwenden oder ändern. Eine gespeicherte Suche ist ein spezieller Filter, der eine dynamische Liste von Computern anzeigt, die die Filterkriterien erfüllen. Sie können auch eine ganz neue gespeicherte Suche erstellen.

Siehe "Info zur Ansicht "Computer" " auf Seite 36.

Die Liste Alle Computer stellt den Startpunkt dar, von dem alle Computer und alle gespeicherten Suchen angezeigt werden.

So suchen Sie nach einem Computer und speichern die Suche als Filter

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Computer".
2. Geben Sie im Listenbereich den vollständigen Name oder einen Teil des Namens eines Computers in das Suchfeld ein.

Vollständiger Name	Geben Sie den vollständigen Namen eines bestimmten Computers oder einer Gruppe von Computern ein, die Sie finden möchten.
Teilweiser Name	Geben Sie einen teilweisen Namen ein, wenn die Suche alle Computer liefern soll, deren Namen eine bestimmte Zeichenkette enthalten. Um alle Computer mit einer Ortsangabe wie Indien als Namenspräfix anzuzeigen, können Sie Ind eingeben. In den Suchergebnissen werden alle Computer angezeigt, die diese Zeichenkette enthalten.

3. (Optional) Um erweiterte Suchfunktionen zu verwenden, klicken Sie auf den Pfeil nach unten neben dem Suchfeld, und wählen Sie dann das Suchkriterium aus, das Sie anwenden möchten.

   Siehe "Info zu Suchoperatoren" auf Seite 45.

4. (Optional) Um mehrere Suchkriterien auszuwählen, klicken Sie neben der Dropdown-Liste "Suchkriterien hinzufügen" auf den Pfeil nach unten, wählen Sie ein Kriterium aus und wiederholen Sie dann den Schritt, um andere Kriterien hinzuzufügen.

   Um ein Suchkriterium zu entfernen, lassen Sie das Feld leer.

5. (Optional) Wenn die Kriterien, die Sie verwenden möchten, nicht in der Dropdown-Liste der erweiterten Suche aufgelistet wird, erstellen Sie benutzerdefinierte Suchkriterien. Um ein benutzerdefiniertes Suchkriterium zu erstellen, führen Sie folgende Schritte durch:

   - Klicken Sie im Listenbereich neben dem Suchfeld auf den Pfeil nach unten.
   - Klicken Sie in der Dropdown-Liste "Suchkriterien hinzufügen" auf "Benutzerdefinierte Kriterien hinzufügen".
   - Aktivieren Sie im Dialogfeld "Suchkriterien hinzufügen" die Datenklassen und Spalten, die Sie als Suchkriterien verwenden möchten.
     Beachten Sie, dass durch das Auswählen der Spalten die Suchkriterien in der Dropdown-Liste aufgefüllt und die zusätzlichen Kriterien als Teil Ihrer Suche verfügbar werden.
   - Klicken Sie auf "OK".

6. Klicken Sie zum Speichern der Suche auf das Speichersymbol im Bereich der erweiterten Suche.

   Beachten Sie, dass jedes Feld, das keinen Wert enthält, in der Abfrage ignoriert und nicht gespeichert wird, wenn Sie die Suche sichern.

7. Geben Sie im Dialogfeld "Suche speichern" im Feld "Name" einen Namen ein und klicken Sie auf "OK".

   Die gespeicherte Suche wird unter "Gespeicherte Suchvorgänge" im Navigationsfenster angezeigt und ist zur Wiederverwendung verfügbar.

8. (Optional) Wenn Sie eine gespeicherte Suche nur als Filter für Aufträge, Aufgaben oder Richtlinien verwenden möchten und sie nicht im Navigationsbereich angezeigt werden soll, können Sie sie auch verbergen. Um die gespeicherte Suche zu verbergen, führen Sie folgende Schritte durch:

   - Klicken Sie mit der rechten Maustaste auf "Gespeicherte Suchvorgänge" und klicken Sie dann auf "Gespeicherte Suchvorgänge verwalten".
   - Deaktivieren Sie im Dialogfeld "Gespeicherte Suchvorgänge verwalten" das Feld neben der Suche, die nicht angezeigt werden soll.
   - Klicken Sie auf "Schließen".

Video: Weitere Informationen zum Erstellen von erweiterten gespeicherten Suchen in den erweiterten Ansichten finden Sie in dem Video Erstellen erweiterter gespeicherter Suchvorgänge in Enhanced Console Views auf Symantec Connect.

Über die Ansicht "Software"

Hinweis: Eine der folgenden Lösungen oder Suites muss installiert sein, damit diese Seite angezeigt wird: Deployment Solution (eigenständiges Produkt), IT Management Suite, Server Management Suite oder Client Management Suite.

Um auf die erweiterte Ansicht "Software" zuzugreifen, klicken Sie in der Symantec Management Console auf "Verwaltung > Software".

Die Ansicht "Software" bietet drei Teilfenster: Navigationsbereichauf der linken Seite, eine Liste der Software und ein Suchfeld in der Mitte und ein Inhaltsbereich auf der rechten Seite. Der Navigationsbereich enthält gespeicherte Suchvorgänge. Der Listenbereich zeigt die Software-Elemente von dem ausgewählten gespeicherten Suchvorgang an. Der Inhaltsbereich zeigt die Details über die Software an, die Sie auswählen.

Mit der Ansicht "Software" können Sie folgende Aufgaben durchführen:

- Suchen von Software geordnet nach Name, Hersteller oder anderen Kriterien. Siehe "Suchen nach Software und Speichern der Suche" auf Seite 41.
- Verwalten von Softwareprodukten.
- Installieren von Software per Drag and Drop.
- Verwalten von Softwarelizenzen.
- Nachverfolgen von Softwareverwendung und -lizenzen.

Video: Weitere Informationen zum Verwalten von Software in den erweiterten Ansichten finden Sie in dem Video Importieren von Software mithilfe von Enhanced Console Views, Verwalten importierter Software mithilfe von Enhanced Console Viewsund Bereitstellen von Software mithilfe von Enhanced Console Views auf Symantec Connect.

Suchen nach Software und Speichern der Suche

In der erweiterten Ansicht "Software" werden die Suchergebnisse, die im Listenbereich angezeigt werden, nicht automatisch gefiltert. Sie können die Suche und die erweiterten Suchfunktionen verwenden, um Ihre Liste einzugrenzen und weiter zu verfeinern, bis der Listenbereich die entsprechende Software enthält.

Siehe "Über die Ansicht "Software" " auf Seite 41.

Sie können die benutzerdefinierte Softwaresuche speichern und später wiederverwenden. Gespeicherte Suchvorgänge werden im Navigationsbereich, im Unterfenster "Installierte Software" angezeigt. Sie können die gespeicherten Suchvorgänge als Filter verwenden, um auf Software, Aufgaben, Aufträge und Richtlinien zugreifen zu können. Mit gespeicherten Suchvorgängen ist auch die Verteilung von Software auf bestimmten Computern oder Computergruppen möglich.

So suchen Sie nach einer bestimmten Software suchen und speichern die Suche

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Software".
2. Klicken Sie im Navigationsbereich auf eine gespeicherten Suchvorgang, den Sie als Startpunkt Ihrer Suche verwenden möchten.
3. Geben Sie im Listenbereich in das Suchfeld die Suchkriterie ein.
4. (Optional) Um erweiterte Suchfunktionen zu verwenden, klicken Sie auf den Pfeil nach unten neben dem Suchfeld, und wählen Sie dann das Suchkriterium aus, das Sie anwenden möchten.

   Siehe "Info zu Suchoperatoren" auf Seite 45.
5. (Optional) Um mehrere Suchkriterien auszuwählen, klicken Sie neben der Dropdown-Liste auf den Pfeil nach unten, wählen Sie ein Kriterium aus und wiederholen Sie dann den Schritt, um andere Kriterien hinzuzufügen.
6. (Optional) Wenn die Kriterien, die Sie verwenden möchten, nicht in der Dropdown-Liste der erweiterten Suche aufgelistet wird, erstellen Sie benutzerdefinierte Suchkriterien. Um ein benutzerdefiniertes Suchkriterium zu erstellen, führen Sie folgende Schritte durch:
   - Klicken Sie in der Dropdown-Liste "Suchkriterien hinzufügen" auf "Benutzerdefinierte Kriterien hinzufügen".
   - Aktivieren Sie im Dialogfeld "Suchkriterien hinzufügen" die Datenklassen und Spalten, die Sie als Suchkriterien verwenden möchten.
     Beachten Sie, dass durch das Auswählen der Spalten die Suchkriterien in der Dropdown-Liste aufgefüllt und die zusätzlichen Kriterien als Teil Ihrer Suche verfügbar werden.
   - Klicken Sie auf "OK".
7. Klicken Sie zum Speichern der Suche auf das Speichersymbol im Bereich der erweiterten Suche.

   Beachten Sie, dass jedes Feld, das keinen Wert enthält, in der Abfrage ignoriert und nicht gespeichert wird, wenn Sie die Suche speichern.

8 Geben Sie im Dialogfeld "Suche speichern" im Feld "Name" einen Namen ein und klicken Sie auf "OK".

Die gespeicherte Suche wird unter "Installierte Software" im Navigationsbereich angezeigt und ist zur Wiederverwendung verfügbar.

9 (Optional) Wenn Sie eine gespeicherte Suche nur als Filter für Aufträge, Aufgaben oder Richtlinien verwenden möchten und sie nicht im Navigationsbereich angezeigt werden soll, können Sie sie auch verbergen. Um die gespeicherte Suche zu verbergen, führen Sie folgende Schritte durch:

- Klicken Sie mit der rechten Maustaste auf "Installierte Software" und dann auf "Gespeicherte Suchvorgänge verwalten".
- Deaktivieren Sie im Dialogfeld "Gespeicherte Suchvorgänge verwalten" das Feld neben der Suche, die nicht angezeigt werden soll.
- Klicken Sie auf "Schließen".

Informationen zum Fenster Softwarekatalog

Hinweis: Eine der folgenden Lösungen oder Suites muss installiert sein, damit diese Seite angezeigt wird: Deployment Solution (eigenständiges Produkt), IT Management Suite, Server Management Suite oder Client Management Suite.

Das Fenster "Softwarekatalog" erscheint innerhalb der Ansicht "Software".

Um auf das Fenster "Softwarekatalog" zuzugreifen, klicken Sie in der Symantec Management Console auf "Verwaltung > Softwarekatalog". Sie können auch zu "Verwaltung > Software" navigieren, mit der rechten Maustaste auf "Installierte Software" klicken und anschließend auf "Softwarekatalog verwalten" klicken.

Siehe "Über die Ansicht "Software" " auf Seite 41.

Im Fenster "Softwarekatalog" können Sie die folgenden Software-Verwaltungsaufgaben durchführen:

- Importieren Sie oder fügen Sie neue Softwarekomponenten und Softwareprodukte hinzu.
  Sie können Software importieren, selbst wenn es nicht im Inventar gefunden wird.
- Hinzufügen neu erkannter bzw. nicht definierter Software, die Sie verwalten möchten, zu Ihrer Liste verwalteter Software.
- Verschieben neu erkannter bzw. nicht definierter Software, die Sie nicht verwalten möchten, in Ihre Liste nicht verwalteter Software.

- Verschieben Sie bei Bedarf Softwareprodukte von einer Liste in eine andere Liste.
- Löschen Sie ein Softwareprodukt. Diese Aktion bricht die Zuordnung zwischen Softwarekomponenten und den Paketen ab, durch die sie bereitgestellt wurden. Wenn Sie ein Softwareprodukt löschen, werden seine Komponenten erneut im Teilfenster "Neu erkannte bzw. nicht definierte Software" aufgeführt.

Informationen zur Ansicht Jobs/Aufgaben

Hinweis: Eine der folgenden Lösungen oder Suites muss installiert sein, damit diese Ansicht angezeigt wird: Deployment Solution (eigenständiges Produkt), IT Management Suite, Server Management Suite oder Client Management Suite.

Um in der Symantec Management Console auf die Ansicht "Aufträge/Aufgaben" zuzugreifen, klicken Sie auf "Verwaltung > Aufträge und Aufgaben".

Mit der Ansicht "Aufträge/Aufgaben" können Sie alle verfügbaren Aufträge und Aufgaben anzeigen und bearbeiten. Beispielsweise können Sie Aufträge und Aufgaben ausführen, indem Sie sie per Drag and Drop auf einen oder mehrere Computer ziehen. Sie können auch die Option "Schnellausführung" verwenden, um einen Auftrag oder eine Aufgabe ohne einen manuellen Drilldown zu bearbeiten.

Siehe "Ausführen eines Auftrags oder einer Aufgabe mit Drag & Drop" auf Seite 441.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

Informationen zur Ansicht Richtlinien

Hinweis: Eine der folgenden Lösungen oder Suites muss installiert sein, damit diese Seite angezeigt wird: Deployment Solution (eigenständiges Produkt), IT Management Suite, Server Management Suite oder Client Management Suite.

Um auf die erweiterte Ansicht "Richtlinien" zuzugreifen, klicken Sie in der Symantec Management Console auf "Verwaltung > Richtlinien".

Mit der erweiterten Ansicht "Richtlinien" können Sie alle verfügbaren Richtlinien anzeigen und bearbeiten. Sie können alle üblichen Funktionen zum Anwenden von Regeln und Reparaturen auf Computern ausführen. Sie können die Zeitpläne für die Überprüfung der Richtlinieneinhaltung einstellen und Richtlinien aktivieren. Sie können Richtlinien starten, indem Sie sie per Drag and Drop auf einen oder mehrere Computer ziehen. Sie können auch die Option "Schnellzuordnung" verwenden, um eine Richtlinie ohne einen manuellen Drilldown zu bearbeiten.

Siehe "Anwenden eine Richtlinie mit Drag and Drop" auf Seite 395.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

Info zu Suchoperatoren

Sie können die Suchoperatoren verwenden, um die Ergebnisse einzuschränken, wenn Sie nach einem bestimmten Element oder einer Gruppe von Elementen suchen.

Siehe "Suchen nach einem Computer und Speichern der Suche als Filter" auf Seite 39.

Siehe "Suchen nach Software und Speichern der Suche" auf Seite 41.

Es gelten die folgenden allgemeinen Suchbedingungen:

- Anführungszeichen begrenzen die Suche auf eine genaue Übereinstimmung.
  Windows XP = Computer, die GENAU - Übereinstimmung Windows XP ausführen.
  "Adobe Acrobat" = computers running EXACT MATCH Adobe Acrobat.
- Weglassen von Anführungszeichen ermöglicht die Suche nach Zeichenketten in Texten.
  Windows XP = computers running LIKE Windows XP anywhere in the name.
  Adobe Acrobat = computers running LIKE Adobe Acrobat anywhere in the name.

Tabelle 2-3 Suchoperatoren, die Sie verwenden können, um verschiedene Argumente auszudrücken

Argument	Symbol	Beschreibung
Oder	Pipe-Symbol (|).	Dieser Operator erfordert keine führenden Leerstellen. Beispiele für die Syntax zum Suchen nach einem Computer: ■ Windows|XP = Computer, die "WIE" Windows ODER "WIE" XP ausführen ■ XP|2000|2003 = Computer, die "WIE" XP ODER "WIE" 2000 ODER "WIE" 2003 ausführen Beispiele für die Syntax zum Suchen nach einer Software: ■ Adobe|Microsoft = software manufacturer LIKE Adobe OR LIKE Microsoft

Argument	Symbol	Beschreibung
Und, Hinzufügen oder Einschließen	Pluszeichen (+).	Dieser Operator erfordert kein führendes Leerzeichen. Beispiele für die Syntax zum Suchen nach einem Computer: ■ Windows+XP = Computer, die "WIE" Windows "UND" XP ausführen ■ Windows+2008 = Computer, die XP "WIE" Windows "UND" 2008 ausführen Beispiele für die Syntax zum Suchen nach einer Software: ■ Adobe+Microsoft = software manufacturer LIKE Adobe AND Microsoft
Nicht, Minus oder Nicht einschließen	Minuszeichen (-).	Dieser Operator erfordert ein führendes Leerzeichen. Wenn Sie ein Minuszeichen ohne führendes Leerzeichen einfügen, wird er nicht als Operator interpretiert. Als optimales Verfahren empfiehlt sich, mit der allgemeinen Gruppe zu beginnen, in der Sie suchen möchten, und dann den auszuschließenden Text einzugeben. Beispiele für die Syntax zum Suchen nach einem Computer: ■ Windows [space] -XP = computers running Windows NOT LIKE XP ■ Windows Server [space] -2003 = computers running Windows Server NOT LIKE 2003 Die folgenden Beispiele setzen voraus, dass Ihre Computer mit Ziffern benannt sind (z. B. pc-1, pc-12, pc-27, pc-125, pc-218, pc-243 und pc-321): ■ PC [Leerzeichen] -1 = Computer namens PC NICHT "WIE" 1, 12, 125, 218, 321 ■ PC [Leerzeichen] -1 = Computer namens PC NICHT "WIE" 27, 12, 125, 218, 321 Beispiele für die Syntax zum Suchen nach einer Software: ■ -Adobe -Microsoft = software manufacturer NOT LIKE Adobe and NOT LIKE Microsoft

Konfigurieren der erweiterten Ansichten

Mit den erweiterten Ansichten in Symantec Management Console können Sie bestimmte Einstellungen konfigurieren. Sie können bestimmte Suchfelder so konfigurieren, dass Sie Ihre Ergebnisse bei der Eingabe der Parameter sehen können. Sie können dieselben Suchfelder auch so konfigurieren, dass Sie Ihre Ergebnisse erst nach dem Drücken der **Eingabetaste** sehen. Sie können die erweiterten Ansichten so konfigurieren, dass sie IME (Input Method Editor) verwenden, damit Sie Doppelbyte-Zeichen in diesen Ansichten eingeben können. Sie können auch die Anzahl von Computern und Softwareprodukten konfigurieren,

die in der Ergebnisliste angezeigt werden. Wenn Sie eine sehr große Anzahl von Computern verwalten, kann diese Einstellung die Ladezeit verkürzen.

So konfigurieren Sie die Einstellungen für die erweiterten Ansichten

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Konsole > Erweiterte Ansichten".
2. Im Dialogfeld "Einstellungen der erweiterten Ansichten" konfigurieren Sie die folgenden Einstellungen:

Suche	"Beim Tippen" - Diese Option ermöglicht die Anzeige der Ergebnisse bei der Eingabe der Anforderungen in das Suchfeld. Die Standardeinstellung ist "Beim Tippen". "Nach dem Drücken der Eingabetaste" - Diese Option zeigt die Ergebnisse erst nach Eingabe der Anforderungen in das Suchfeld und Drücken der **Eingabetaste** an. Diese Suchoptionen betreffen die folgenden Suchfelder: ■ Ansicht "Computer", mittleres Suchfeldteilfenster, das alle gespeicherten und gefilterten Suchen enthält ■ Ansicht "Software", mittleres Suchfeldteilfenster, das alle gespeicherten und gefilterten Suchen enthält
IME (Input Method Editor) für die Eingabe von Doppelbyte-Zeichen zulassen	Aktiviert IME-Unterstützung für erweiterte Ansichten und für das Portal der Ersteinrichtung. Wenn diese Option aktiviert ist, können Sie IME verwenden, um Doppelbyte-Zeichen auf diesen Seiten einzugeben.

Computer und Software-Ergebnisliste beschränken auf	Begrenzt die Anzahl von Computern oder Softwareprodukten, die in einer Ergebnisliste angezeigt werden können. Wenn Ihre Umgebung eine Hierarchie mit Tausenden von Computern hat, kann das Laden der Listen lange dauern und es kann sogar zu einer Zeitüberschreitung kommen. Diese Begrenzung legt fest, wie viele Zeilen die Abfrage ausgeben sollte. Die Standardeinstellung ist 20.000, aber Sie können diese Einstellung heruntersetzen, um Ladezeiten zu verkürzen. Wenn zusätzliche Zeilen vorhanden sind, gibt die letzte Zeile an, dass es mehr Datensätze gibt und ermöglicht das Laden dieser Datensätze.

3 Klicken Sie auf "OK".

Aufrufen der Symantec Management Console

Symantec Management Console (normalerweise als "die Konsole" bezeichnet) kann vom Computer, der Notification Server ausführt, oder über Fernzugriff aufgerufen werden. Eine Remote-Verbindung macht es erforderlich, dass der Remote-Computer Zugriff auf den Notification Server-Computer hat und eine unterstützte Version von Microsoft Windows und Microsoft Internet Explorer ausführt. Da die Konsole auf dem Internet-Browser basiert, müssen Sie keine spezielle Software installieren, um die Konsole zu verwenden.

Siehe "Info zur Symantec Management Console" auf Seite 33.

Sie müssen ein Mitglied einer oder mehrerer Notification Server-Sicherheitsrollen sein, um die Konsole aufrufen zu können.

Siehe "Infos zur Sicherheit der Symantec Management-Plattform" auf Seite 86.

Hinweis: Die Symantec Management-Plattform unterstützt NTLM-Authentifizierung für Remote-Verbindungen. Dadurch können Sie über einen Remote-Computer Symantec Management Console aufrufen, ohne zur Eingabe von Benutzername und Kennwort aufgefordert zu werden (dies wird manchmal als "Einzel-Login" an der Konsole bezeichnet). Sie müssen am Remote-Computer mit einem Symantec Management-Plattform-Konto eingeloggt sein, und Sie sollten den vollständig qualifizierten Domänennamen (FQDN) für den Notification Server-Namen verwenden.

Wenn Sie beim Herstellen der Verbindung zu Symantec Management Console zur Eingabe von Benutzername und Kennwort aufgefordert werden, müssen Sie unter Umständen den Notification Server-Namen (FQDN) der Zone "Vertrauenswürdige Sites" auf dem Remote-Computer hinzufügen. Dies erfolgt in der Systemsteuerung im Dialogfeld "Internetoptionen" auf der Registerkarte "Sicherheit".

Die Konsole unterstützt die 32-Bit-Version von Microsoft Internet Explorer 7.0. Es werden nur 32-Bit-ActiveX-Steuerelemente verwendet. Daher werden 64-Bit-Browser nicht unterstützt. Wenn Sie die Konsole mit einem nicht unterstützten Browser öffnen, wird eine Meldung in der oberen Zeile angezeigt. Die Meldung warnt Sie, dass der Browser nicht unterstützt wird und dass einige Funktionen möglicherweise nicht zur Verfügung stehen. Sie verwenden nicht unterstützte Browser auf eigenes Risiko.

Einige Active-X-Steuerelemente müssen installiert werden, damit die Konsole ordnungsgemäß funktioniert. Sie benötigen ein Administratorkonto auf dem Konsolencomputer. Sie können auch Ihren IT-Support bitten, die entsprechenden Active-X-Steuerelemente zu installieren.

Hinweis: Wenn Probleme auftreten (z. B. Konsolenseiten mit Fehlermeldungen, verlorene Daten oder UI-Steuerelemente, die sich unerwartet verhalten), stellen Sie sicher, dass der Name des angegebenen Notification Server richtig ist. Der Name des Notification Server darf nur alphanumerische Zeichen enthalten Sonderzeichen, einschließlich Unterstrichen, sind nicht zulässig.

So greifen Sie lokal auf die Symantec Management Console zu

- Wählen Sie auf dem lokalen Computer im Menü "Start" die Optionen "Programme > Symantec > Symantec Management Console".

So greifen Sie per Fernzugriff auf Symantec Management Console zu

1 Öffnen Sie auf dem Remote-Computer Internet Explorer und rufen folgende URL-Adresse auf:

http://*Name des Notification Server*/altiris/console

Der Notification Server-Name sollte ein vollständig qualifizierter Domänenname sein. Sie können "https" bei Bedarf verwenden. Wenn Notification Server nicht auf Port 80 ist, müssen Sie die entsprechende Portnummer nach dem Notification Server-Namen einfügen.

2 Wenn Sie am Remote-Computer mit einem Konto angemeldet sind, das kein Symantec Management-Plattform-Konto ist, werden Sie zur Eingabe Ihres Benutzernamens und Kennworts aufgefordert.

Wenn Sie am Remote-Computer mit einem Symantec Management-Plattform-Konto angemeldet sind, übernimmt die Einzel-Login-Funktion dieses automatisch. Wenn die Eingabeaufforderung erscheint, müssen Sie unter Umständen den Notification Server-Namen (FQDN) der Zone "Vertrauenswürdige Sites" auf dem Remote-Computer hinzufügen.

Aufrufen der Dokumentation in der Symantec Management Console

Es gibt zwei Möglichkeiten, auf die Dokumentation innerhalb von Symantec Management Console zuzugreifen: die kontextbezogene Hilfe und die Dokumentationsbibliothek. Die kontextbezogene Hilfe erlaubt den Zugriff auf Informationen zu dem gerade aktiven Bereich in der Konsole (Seite, Dialogfeld oder Registerkarte). Im Rahmen der kontextbezogenen Hilfe wird das Benutzerhandbuch, das sich auf den aktiven Bereich bezieht, in einem neuen Fenster geöffnet.

Die Dokumentationsbibliothek ist eine Seite in der Symantec Management Console, über die Sie die Dokumentation zu den einzelnen installierten Produkten (Benutzerhandbücher, Administratorhandbücher, Implementierungshandbücher und Versionshinweise) aufrufen können. Die Dokumentation kann sich, wie im Falle der Benutzerhandbücher, auf dem Notification Server-Computer oder, wie bei den Versionshinweisen, auf einer Website befinden. Da die Dokumentation teilweise im Adobe-Acrobat-Format vorliegt, benötigen Sie Adobe Acrobat Reader, um die Seiten anzuzeigen oder zu drucken.

Siehe "Info zur Symantec Management Console" auf Seite 33.

So greifen Sie auf die kontextbezogene Hilfe zu

1. Vergewissern Sie sich, dass der Bereich in Symantec Management Console, auf den Sie zugreifen möchten, aktiv ist.

   Um einen Bereich zu aktivieren, klicken Sie an eine beliebige Stelle. Bei einer Seite oder einem Dialogfeld klicken Sie einfach darauf.
2. Führen Sie einen der folgenden Schritte durch:
   - Wählen Sie im Menü "Hilfe" die Option "Kontext".
   - Drücken Sie die Taste **F1**.

So greifen Sie auf die Dokumentationsbibliothek zu

1. Wählen Sie in der Symantec Management Console im Menü "Hilfe" die Option "Dokumentationsbibliothek".
2. Klicken Sie auf der Seite "Dokumentationsbibliothek" auf den Link zur gewünschten Dokumentation.

Aufrufen der Seite "Mein Portal"

Die Seite "Mein Portal" ist die Standardseite, wenn ein neuer Benutzer die Symantec Management Console öffnet.

Vom Benutzer vorgenommene Änderungen an der Seite "Mein Portal" (z. B. Hinzufügen, Bearbeiten oder Entfernen von Web-Parts) gelten nur für diesen Benutzer und werden unter seiner Benutzer-ID gespeichert. Wenn sich der Benutzer anmeldet und im Menü "Konsole" die Option "Seite "Mein Portal"" auswählt, wird seine angepasste Seite "Mein Portal" automatisch geladen.

Siehe "Erstellen und Ändern von Portalseiten" auf Seite 59.

So rufen Sie die Seite "Mein Portal" auf

- Wählen Sie in der Symantec Management Console im Hauptmenü die Option "Mein Portal".

Zugreifen auf die Startseite von Notification Server Management

Auf der Startseite von Notification Server Management haben Sie Zugriff auf wichtige Informationen über Notification Server und die installierten Lösungen.

Auf der Startseite von Notification Server Management gibt es folgende Informationen:

Ressourcenmanager	Mit diesem Link können Sie eine Ressource auswählen, um sie in der Ressourcenmanager-Konsole anzuzeigen.
Installierte Produkte	Liste der auf Notification Server installierten Lösungen.
Site Server	Liste der Site Services und Site Servern der Website von Notification Server.
Hierarchie	Ausführliche Informationen über die Hierarchie, zu der Notification Server gehört. Diese Informationen werden nur angezeigt, wenn Notification Server zu einer Hierarchie gehört.
Agent-Rolloutstatus	Status des Symantec Management-Agent-Rollouts auf den Computern, die Sie verwalten möchten.
Lizenzen	Für jede Lösung sind folgende Informationen aufgelistet: ■ Gesamtanzahl der verfügbaren Lizenzen ■ Anzahl der verwendeten Lizenzen ■ Ablaufdatum der Lizenz (falls zutreffend)

Wie alle Portalseiten auch kann die Startseite von Notification Server Management benutzerspezifisch angepasst werden. Konfigurieren Sie die Seite mit den für Sie am hilfreichsten Informationen.

Siehe "Erstellen und Ändern von Portalseiten" auf Seite 59.

So öffnen Sie die Startseite von Notification Server Management

- Klicken Sie in Symantec Management Console im Menü "Startseite" auf "Notification Server Management" > "Portal".

Anpassen der Symantec Management Console

Sie können Symantec Management Console den Anforderungen Ihrer Organisation entsprechend anpassen. Beispielsweise empfiehlt es sich, dem Konsolenmenü zusätzliche Untermenüelemente hinzuzufügen, um den Benutzern in Ihrer Organisation zu entsprechen. Sie können Menüoptionen der oberen Ebene nicht ändern und auch keine Untermenüelemente, die von Symantec Management Console bereitgestellt wurden, bearbeiten oder entfernen.

Die meisten benutzerspezifischen Anpassungen erfolgen systemweit. Um einen benutzerspezifische Anpassung auf Rollenebene zu erzielen, können Sie die Sicherheit für Elemente verwenden. Beispielsweise können Sie eine Portalseite erstellen, die nur für eine bestimmte Rolle zugänglich ist. In diesem Fall wird die benutzerspezifische Anpassung mit Berechtigungen für Elemente und nicht für Privilegien implementiert. Ansichten, Verzeichnisstrukturen und Menüs können

auch anhand von Sicherheitseinstellungen benutzerspezifisch angepasst werden. Beispielsweise kann ein Symantec-Administrator die Berechtigung für ein Verzeichnisstrukturelement oder eine Menüoption entsprechend festlegen, so dass Benutzer in einer bestimmten Rolle sie sehen können, aber Benutzer in einer anderen Rolle nicht. Jedoch gilt die Seite "Mein Portal" und die Personalisierung pro Seite jeweils für den Benutzer.

Tabelle 2-4 Anpassungsaufgaben

Aufgabe	Beschreibung
Anpassen von Menüs	Sie können Untermenüs und Untermenüpunkten hinzufügen sowie die Menüstruktur optimieren. Siehe "Anpassen des Konsolenmenüs" auf Seite 54.
Anpassen der Kontextmenüs	Sie können dem Kontextmenü benutzerdefinierte Aktionen hinzufügen. Siehe "Hinzufügen benutzerdefinierter Aktionen zum Kontextmenü" auf Seite 55.
Anpassen der Ansichten	Zum Optimieren der Struktur können Sie Ansichten erstellen und ändern. Siehe "Erstellen und Ändern von Ansichten" auf Seite 57. Siehe "Hinzufügen neuer Elemente direkt zu einer Ansicht" auf Seite 58.
Anpassen von Portalseiten	Erstellen und ändern Sie Portalseiten. Eine Portalseite ist eine Symantec Management Console-Seite, die Sie Ihren Anforderungen entsprechend anpassen können. Sie können eine Portalseite verwenden, um Schlüsselinformationen auf einer einzelnen, überschaubaren Seite zusammenzufassen. Eine Portalseite kann den Status der Symantec Management-Plattform und verwalteten Computer anzeigen oder jegliche andere Informationen, die Sie verfügbar machen möchten. So zum Beispiel können Sie externe Webseiten, Intranetseiten, RSS-Feeds oder Ihre eigenen Anwendungen einfügen. Siehe "Erstellen und Ändern von Portalseiten" auf Seite 59.
Anpassen von Web-Parts	Sie können Web-Parts, die Sie zum Erstellen von Portalseiten verwenden, erstellen und ändern. Siehe "Erstellen und Ändern von Web-Parts" auf Seite 62.

Sie können Ihre angepassten Konsolenelemente als XML-Dateien speichern und sie bei Bedarf wiederherstellen, indem Sie die entsprechenden Dateien importieren.

Siehe "Speichern der Konsolenelemente als XML-Dateien" auf Seite 63.

Anpassen des Konsolenmenüs

Sie können das Konsolenmenü Ihren Anforderungen entsprechend anpassen. Die Menüoptionen, die von der Symantec Management-Plattform bereitgestellt werden, sind schreibgeschützt und können nicht geändert werden. Sie können neue Untermenüs hinzufügen und sie bei Bedarf ändern. Sie können jedes Menüelement verschieben oder löschen, ausgenommen diejenigen, die als schreibgeschützt gekennzeichnet sind.

Siehe "Anpassen der Symantec Management Console" auf Seite 52.

So passen Sie das Konsolenmenü an

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Konsole > Menüs".
2. Führen Sie auf der Seite "Menü bearbeiten" die entsprechenden Aufgaben zur benutzerspezifischen Anpassung durch:

So fügen Sie Menüelemente hinzu	1 Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Menüpunkt, unter dem ein neuer angelegt werden soll, und klicken Sie dann auf "Neues Element". 2 Geben Sie auf der Seite "Menüdetails" die erforderlichen Details an und klicken Sie dann auf "Übernehmen".
So fügen Sie Untermenüs hinzu	1 Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Menüpunkt, unter dem ein Untermenü eingefügt werden soll, und klicken Sie dann auf "Neues Untermenü". 2 Klicken Sie auf "Übernehmen".
So importieren Sie Untermenüelemente aus einer XML-Datei	1 Klicken Sie im linken Teilfenster mit der rechten Maustaste auf das Untermenü, in das Menüpunkte importiert werden sollen, und klicken Sie dann auf "Untermenü importieren". 2 Wählen Sie im Dialogfeld "Wählen Sie die zu importierende XML-Datei" die gewünschte XML-Datei aus und klicken Sie auf "Öffnen". 3 Klicken Sie auf "Übernehmen".

So exportieren Sie ein Untermenü in eine XML-Datei	1 Klicken Sie im linken Teilfenster mit der rechten Maustaste auf das zu exportierende Untermenü und klicken Sie dann auf "Exportieren…". 2 Geben Sie im Dialogfeld "Zieldatei für exportierte XML" den XML-Dateinamen und Speicherort an und klicken Sie auf "Speichern".
So importieren Sie das gesamte Konsolenmenü aus einer XML-Datei:	1 Klicken Sie im linken Teilfenster in der Symbolleiste auf das Symbol "Gesamtes Menü importieren". 2 Wählen Sie im Dialogfeld "Wählen Sie die zu importierende XML-Datei" die gewünschte XML-Datei aus und klicken Sie auf "Öffnen".

Hinzufügen benutzerdefinierter Aktionen zum Kontextmenü

Das Kontextmenü ("Rechtsklick") der Konsole enthält die Menüoptionen, die für Ordner oder Elemente relevant sind, auf die Sie geklickt haben. Standardoptionen für das Kontextmenü ("Rechtsklick") stehen in Notification Server zur Verfügung und weitere Optionen werden unter Umständen durch installierte Lösungen hinzugefügt. Die meisten Standardoptionen sind allgemeine Funktionen, die für die meisten Ordner und Elemente verfügbar sind.

Sie können benutzerdefinierte Aktionen erstellen und in das Kontextmenü übernehmen. Folgende Aktionen sind möglich:

- Öffnen Sie eine URL und ersetzen Sie Details (z. B. den Namen) der ausgewählten Ressource in der URL.
- Führen Sie eine Kommandozeile auf dem Notification Server-Computer oder dem Computer aus, auf dem der Browser ausgeführt wird.

Hinweis: Wenn ein Benutzer Kommandozeilen-Rechtsklickaktionen auf einem Computer ausführen möchte, muss das entsprechende SSL-Zertifikat installiert sein. Sie können das benötigte SSL-Zertifikat von der Seite "Kommandozeilen-Rechtsklickaktionszertifikat" herunterladen.

Sie können die Ressourcen angeben, auf die sich eine Aktion bezieht, indem Sie den Ressourcentyp auswählen und (optional) die Ressourcen durch eine Abfrage

filtern. Wenn Sie mit der rechten Maustaste auf eine Ressource des Typs klicken, der die Filterabfrage erfüllt (falls ein Filter angegeben wurde), enthält das Kontextmenü die benutzerdefinierte Aktion.

Um benutzerdefinierte Aktionen in das Kontextmenü zu übernehmen, ist die Berechtigung für neue Aktionen per Rechtsklick erforderlich.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

So fügen Sie dem Kontextmenü eine benutzerdefinierte Aktion hinzu

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Konsole" > "Rechtsklickaktionen".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, dem Sie die Aktion hinzufügen möchten, und klicken Sie dann auf "Neu" > "Rechtsklickaktion".
3. Geben Sie auf der Seite "Neue Rechtsklickaktion" den Namen und eine Beschreibung ein.
4. Konfigurieren Sie die Aktion anhand folgender Einstellungen:

Aktivieren	Die Aktion muss aktiviert werden, um in das Kontextmenü übernommen zu werden. Die neue Aktion ist standardmäßig deaktiviert. So können Sie die Aktion konfigurieren und testen, bevor sie für andere Konsolenbenutzer freigegeben wird.
Ressourcentyp	Der Ressourcentyp, auf den sich die Aktion bezieht. Standardmäßig sind alle Ressourcen des angegebenen Typs eingeschlossen. Wenn Sie die Aktion auf eine bestimmte Teilmenge der Ressourcen anwenden möchten, können Sie die Ressourcen mit einem Abfrageausdruck filtern.
Aktionstyp	Wählen Sie in der Dropdown-Liste den geeigneten Aktionstyp aus: ■ URL Geben Sie im Feld "Basis-URL" die entsprechende URL an. Die URL kann zu einer anderen Seite in Symantec Management Console oder zu einer externen Intranet- oder Internetsite führen. ■ Kommandozeile Geben Sie im Feld "Kommandozeile" die entsprechende Kommandozeile ein. Aktivieren Sie das Kontrollkästchen "Auf folgendem Server ausführen", um die Kommandozeile vom Server auszuführen. Wenn Sie das Kontrollkästchen deaktiviert lassen, wird die Kommandozeile auf dem Computer ausgeführt, auf dem die Aktion aufgerufen wird.

Ersatzparameter	Ersatzparameter erlauben die Verwendung einer Variablen in Kommandozeile oder URL. Der Wert wird dann durch den Wert bei Ausführung ersetzt. Beispiel: Ressourcenname, IP-Adresse oder GUID. Für jeden einzuschließenden Ersatzparameter gehen Sie wie folgt vor: 1 Klicken Sie auf "Hinzufügen". 2 Wählen Sie im Fenster "Attribute auswählen" das Attribut aus, das Sie als Parameter verwenden möchten. Klicken Sie dann auf "OK". 3 Geben Sie unter "Parametername" einen geeigneten Namen für den Parameter ein.

5 Klicken Sie auf "Übernehmen".

Siehe "Anpassen der Symantec Management Console" auf Seite 52.

Erstellen und Ändern von Ansichten

Notification Server und Lösungen enthalten definierte Ansichten, die Sie, falls erforderlich, ändern und ausdehnen können. Sie können auch eigene Ansichten erstellen und ändern.

Siehe "Info zu Konsolenansichten" auf Seite 35.

So erstellen oder ändern Sie eine Ansicht:

1 Klicken Sie in Symantec Management Console im Menü "Einstellungen" auf "Konsole > Ansichten".

2 Führen Sie im linken Teilfenster im Ordner "Ansichten" einen der folgenden Schritte aus:

So erstellen Sie eine neue Ansicht:	Klicken Sie mit der rechten Maustaste auf den Ordner, zu dem Sie die Ansicht hinzufügen möchten, und wählen Sie "Neu > Ansicht".
So ändern Sie eine vorhandene Ansicht:	Klicken Sie mit der rechten Maustaste auf die gewünschte Ansicht und wählen Sie "Ansicht bearbeiten".

3 Geben Sie auf der Seite "Ansicht bearbeiten" die passenden Details in den folgenden Feldern an:

"Name"	Der Name der Ansicht.
Beschreibung	Eine Beschreibung der Ansicht.
Portalseite anzeigen	Lässt Sie eine Portalseite auswählen, die mit dem Stammordner der Ansicht verbunden werden soll. Wenn Sie den Stammordner der Ansicht im linken Teilfenster auswählen, wird die angegebene Portalseite im Inhaltsteilfenster angezeigt.
Inhalte dieser Ansicht	Zeigt die Struktur der Ansicht an, die Sie erstellen, und lässt Sie neue Ordner erstellen und Elemente löschen, die Sie nicht anzeigen möchten. Der Inhalt wird alphabetisch sortiert, zuerst Ordner und dann Elemente. Sie können die Struktur nicht ändern.
Verfügbare Elemente:	Zeigt die Baumstruktur der Symantec Management Console an. Sie können Ordner und Elemente auswählen, die in der Ansicht angezeigt werden sollen. So fügen Sie ein Element zur Ansicht hinzu: 1 Wählen Sie in der Dropdown-Liste "Struktur" die Verzeichnisstruktur aus, aus der Sie Elemente auswählen möchten. 2 Erweitern Sie die Verzeichnisstruktur und wählen Sie den Ordner oder das Element aus, das Sie zur Ansicht hinzufügen möchten. 3 Klicken Sie auf "Hinzufügen".

4 Klicken Sie auf "OK".

Hinzufügen neuer Elemente direkt zu einer Ansicht

Sie können neue Ordner, Elementverknüpfungen und Weblinks direkt zu einer Ansicht hinzufügen. Sie können auch neue Ansichten hinzufügen, um eine Hierarchie von Ansichten zu erstellen.

Siehe "Info zu Konsolenansichten" auf Seite 35.

So fügen Sie eine neue Komponente direkt einer Ansicht hinzu

1. Klicken Sie in Symantec Management Console im Menü "Einstellungen" auf "Konsole" > "Ansichten".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, unter dem Sie den neuen Ordner oder das Element hinzufügen und die entsprechende Option auswählen möchten:

"Neu" > "Ordner"	Geben Sie in das Dialogfeld "Neuer Ordner" den neuen Ordnernamen ein, und klicken Sie anschließend auf "Übernehmen".
"Neu" > "Elementverknüpfung"	Wählen Sie im Fenster "Elementverknüpfung bearbeiten" das Element aus, zu dem Sie eine Elementverknüpfung erstellen möchten, und klicken Sie dann auf "OK".
"Neu" > "Weblink"	Geben Sie im Dialogfeld "Weblink-Konfiguration" die URL der Webseite an, zu der Sie einen Link erstellen möchten. Sie können Folgendes optional angeben: ■ Symbol-Image-URL Wenn Sie ein Symbol in der Strukturansicht verwenden möchten, geben Sie die URL zur entsprechenden Image-Datei an. ■ Ziel-Frame Die Standardeinstellung ist "rightPane", der Hauptinhaltsbereich, der üblicherweise als das rechte Teilfenster bekannt ist. Klicken Sie auf "Übernehmen".
"Neu" > "Ansicht"	Erstellen Sie im Fenster "Ansicht bearbeiten" die entsprechende Ansicht. Siehe "Erstellen und Ändern von Ansichten" auf Seite 57.

Erstellen und Ändern von Portalseiten

Eine Portalseite ist eine Symantec Management Console-Seite, die Sie Ihren Anforderungen entsprechend anpassen können. Sie können eine Portalseite verwenden, um Schlüsselinformationen auf einer einzelnen, überschaubaren Seite zusammenzufassen. Eine Portalseite kann den Status der Symantec Management-Plattform und der verwalteten Computer anzeigen oder jegliche andere Informationen, die Sie verfügbar machen möchten. Beispielsweise können Sie externe Webseiten, Intranetseiten, RSS-Feeds oder eigene Anwendungen einfügen.

Dies ist praktischer als eine Reihe unterschiedlicher Konsolenseiten anzuzeigen, um die gewünschten Informationen zu erfassen.

Siehe "Anpassen der Symantec Management Console" auf Seite 52.

Die meisten Portalseiten stehen allen Konsolenbenutzern zur Verfügung. Die Ausnahme ist die Seite "Mein Portal", die für jeden Benutzer eindeutig ist.

Siehe " Aufrufen der Seite "Mein Portal"" auf Seite 51.

Hinweis: Um eine Portalseite anzuzeigen, benötigen Sie Leseberechtigung auf dieser Portalseite.

Portalseiten werden mit Web-Parts erstellt. Sie können Web-Parts entsprechend Ihren Anforderungen erstellen bzw. benutzerspezifisch anpassen und sie Ihren Portalseiten hinzufügen.

Es gibt folgende Typen von Web-Parts:

Bericht	Zeigt die Informationen an, die von einem Bericht abgerufen werden.
URL	Ein Link zu einer anderen Webseite (wie beispielsweise eine Seite in Ihrem Unternehmens-Intranet oder eine externe Website).

Portalseiten können bis zu drei Spalten breit sein. Web-Parts können auf einer Portalseite in drei verschiedenen Größen angezeigt werden, je nachdem, in welcher Spalte sie sich befinden oder ob sie alle Spalten umfassen. Die linken und mittleren Spalten haben die gleiche Breite (Web-Parts sind darin "klein"), aber die rechte Spalte ist breiter (Web-Parts sind hier "groß"). Alternativ kann ein Web-Part die gesamte Seitenbreite verwenden (Web-Part ist "mehrspaltig"). Diese mehrspaltigen Web-Parts werden oben oder unten auf der Portalseite gezeigt. Wenn Sie neue Web-Parts entwickeln, müssen Sie sicherstellen, dass sie jeder Größe entsprechend anzeigt werden. Sie können nicht eine bestimmte Größe als Web-Part-Eigenschaft festlegen.

Sie können Web-Parts reduzieren, indem Sie auf den Pfeil oben rechts klicken, und erweitern, indem Sie erneut auf den Pfeil klicken. Dadurch können langsam zu ladende oder selten verwendete Web-Parts auf einer Portalseite enthalten sein.

Portalseiten haben die folgende beiden Betriebsmodi:

Ansicht	Die Portalseite ist schreibgeschützt. Sie können alle Web-Parts anzeigen, aber keine Änderungen vornehmen. Einige Portalseiten, die von Symantec-Lösungen zur Verfügung gestellt werden, sind unter Umständen auf den Ansichtsmodus beschränkt, um Andere am Ändern des Inhalts zu hindern.

Bearbeiten	Wenn Sie Schreibberechtigung auf der Portalseite haben, können Sie sie bearbeiten. Sie können Web-Parts auf einer Portalseite hinzufügen, entfernen, ihre Größe neu bestimmen und sie neu anordnen. Die Web-Parts-Verzeichnisstruktur wird links auf der Seite angezeigt, damit Sie Web-Parts per Drag und Drop an den entsprechenden Orten ablegen können. Um Web-Parts von einer Portalseite zu entfernen, klicken Sie auf das X-Symbol in der rechten oberen Ecke der Web-Parts.

Siehe "Erstellen und Ändern von Web-Parts" auf Seite 62.

So erstellen oder ändern Sie eine Portalseite

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Konsole" > "Portalseiten".
2. Führen Sie einen der folgenden Schritte durch:

So erstellen Sie eine neue Portalseite	Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner "Portalseiten", und wählen Sie im Kontextmenü die Option "Neu" > "Portalseite".
So ändern Sie eine vorhandene Portalseite	Wählen Sie im linken Teilfenster im Ordner "Portalseiten" die zu bearbeitende Seite aus. Klicken Sie in der rechten oberen Ecke der Portalseite auf "Bearbeiten".

3. Geben Sie auf der Seite "Portalseitenkonfiguration" den Namen und die Beschreibung der Seite an, und wählen Sie die Web-Parts aus, die Sie auf der Portalseite verwenden möchten.

Name	Der Name der Portalseite.
Beschreibung	Eine Beschreibung der Portalseite.
Fenster "Web-Parts"	Dieses Fenster enthält die Liste der verfügbaren Web-Parts, die Sie der Portalseite hinzufügen können. So fügen Sie Web-Parts hinzu 1. Wählen Sie den Web-Part aus, und klicken Sie anschließend auf "Hinzufügen". 2. Klicken Sie auf der Portalseite auf den Web-Part, klicken Sie auf den Internet-Teil und ziehen ihn zum entsprechenden Standort auf der Seite.

4 Wenn Sie Web-Parts von der Seite entfernen möchten, klicken Sie im entsprechenden Web-Part-Frame auf das Symbol "Löschen" in der rechten oberen Ecke.

5 Klicken Sie auf "Übernehmen".

Erstellen und Ändern von Web-Parts

Web-Parts sind Mini-Webseiten, die Sie als Bausteine für Portalseiten verwenden können. Ein Web-Part kann einen Bericht oder den Inhalt einer Webseite anzeigen. Die Konsole wird mit einem Satz vordefinierter Web-Parts bereitgestellt, die Sie zum Erstellen Ihrer Portalseiten verwenden können. Sie können diese Web-Parts ändern und auch neue erstellen.

Siehe "Erstellen und Ändern von Portalseiten" auf Seite 59.

Sie können auch einen Bericht für einen Web-Part direkt von einem Bericht erstellen.

Siehe "Speichern von Notification Server-Berichtsergebnissen als Web-Part" auf Seite 469.

So erstellen oder ändern Sie Web-Parts

1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Konsole" > "Web-Parts".

2 Führen Sie einen der folgenden Schritte durch:

So erstellen Sie neue Web-Parts	Erweitern Sie im linken Teilfenster den Ordner "Web-Parts", und klicken Sie mit der rechten Maustaste auf den Ordner, in dem Sie den neuen Web-Part hinzufügen möchten. Klicken Sie auf "Neu" > "Web-Part".
So ändern Sie vorhandene Web-Parts	Erweitern Sie im linken Teilfenster den Ordner "Web-Parts", und wählen Sie den Web-Part aus, den Sie ändern möchten.

3 Geben Sie auf der Seite "Web-Part-Konfiguration" die Web-Part-Parameter an:

Name	Der Name des Web-Parts.
Beschreibung	Eine Beschreibung des Web-Parts.

Web-Part-Inhalt	Der Inhalt des Web-Parts. Sie können eine der folgenden Optionen auswählen: ■ Ergebnisse aus Bericht Wenn Sie diese Option auswählen, müssen Sie den entsprechenden Bericht auswählen. Der Bericht wird ausgeführt, wenn Sie eine Portalseite öffnen, die den Web-Part enthält. Somit sind die Ergebnisse immer aktuell. ■ URL anzeigen Wenn Sie diese Option auswählen, geben Sie die entsprechende URL-Adresse an.
Feste Höhe	Aktivieren Sie diese Option, um eine feste Höhe für den Web-Part anzugeben, und geben Sie anschließend die Höhe (in Pixeln) in das benachbarte Feld ein. Wenn diese Option nicht ausgewählt wird, wird die Größe des Web-Parts entsprechend dem von ihm angezeigten Inhalt geändert.
Standardgröße	Die Standardgröße des Web-Parts: ■ Klein ■ Groß ■ Mehrspaltig Wenn der Web-Part einer Portalseite hinzugefügt wird, wird seine Standardposition durch seine Standardgröße festgelegt. Wenn Sie den Web-Part an eine andere Position verschieben möchten, wird seine Größe automatisch geändert.

4 Wenn Sie die Änderungen abbrechen möchten, ohne etwas zu speichern, klicken Sie auf "Abbrechen".

5 Klicken Sie auf "Änderungen speichern".

6 Wenn Sie den von Ihnen angegebenen Web-Part in der Vorschau anzeigen möchten, klicken Sie auf "Vorschau anzeigen".

Speichern der Konsolenelemente als XML-Dateien

Sie können Konsolenelemente (Menüelemente, Ansichten, Portalseiten oder Web-Parts) als XML-Dateien speichern. Es empfiehlt sich, dies zu tun, um Backup-Dateien zu erstellen, bevor Sie die Konsole anpassen. Sie könnten dies auch tun, um XML-Dateien zu erstellen, die Sie anpassen und als benutzerdefinierte Konsolenelemente in andere Notification Server importieren können.

Siehe "Anpassen der Symantec Management Console" auf Seite 52.

Um Konsolenelemente wiederherzustellen, importieren Sie sie aus den entsprechenden XML-Dateien. Konsolenelemente werden anhand ihrer GUIDs identifiziert. Elemente in der importierten XML-Datei überschreiben vorhandene Elemente, die entsprechende GUIDs haben. Alle Elemente in der XML-Datei, die keine entsprechenden GUIDs in der Konsole haben, werden als neue Objekte hinzugefügt.

Hinweis: Sie benötigen das Privileg "XML importieren", um XML-Dateien zu importieren. Standardmäßig hat nur die Rolle "Symantec-Administrator" dieses Privileg.

So speichern Sie Konsolenelemente als XML-Datei

1. Klicken Sie in der Symantec Management Console im linken Teilfenster auf den Strukturknoten, der gespeichert werden soll.
2. Klicken Sie mit der rechten Maustaste, und klicken Sie dann auf "Exportieren".
3. Geben Sie im Dialogfeld "Zieldatei für exportierte XML" den Namen und Speicherort der XML-Datei an, und klicken Sie dann auf "Speichern".

So stellen Sie ein Konsolenelement aus einer XML-Datei wieder her

1. Wählen Sie in der Symantec Management Console im linken Teilfenster den Ordner, in dem das Element wiederhergestellt werden soll.
2. Klicken Sie mit der rechten Maustaste, und klicken Sie dann auf "Importieren".
3. Wählen Sie im Dialogfeld "Wählen Sie die zu importierende XML-Datei" die entsprechende XML-Datei aus.
4. Wenn Sie jegliche Änderungen am importierten Element vermeiden möchten, aktivieren Sie "Schreibgeschützt öffnen".
5. Klicken Sie auf "Öffnen".

Abschnitt 2

Einrichten der Symantec Management-Plattform-Server

- Kapitel 3. Konfigurieren von Notification Server
- Kapitel 4. Konfigurieren der Sicherheit
- Kapitel 5. Konfigurieren von Zeitplänen
- Kapitel 6. Konfigurieren von Sites und Site Servers
- Kapitel 7. Konfigurieren der Package Server für Linux
- Kapitel 8. Konfigurieren der Hierarchie
- Kapitel 9. Konfigurieren der Replikation
- Kapitel 10. Erstmalige Konfiguration

Kapitel 3

Konfigurieren von Notification Server

In diesem Kapitel werden folgende Themen behandelt:

- Informationen zum Notification Server
- Info zum Konfigurieren von Notification Server
- Konfigurieren von Notification Server-Einstellungen
- Konfigurieren von Notification Server-Einstellungen mit NS Configurator
- Konfigurieren von Configuration Management Database
- Bereinigen der Configuration Management Database
- Speichern des Ressourcendatenverlaufs in der CMDB

Informationen zum Notification Server

Notification Server ist die Primärserverkomponente innerhalb der Symantec Management-Plattform. Notification Server koordiniert die verschiedenen Lösungen und liefert die Primärbenutzeroberfläche, die richtlinienbasierte Verwaltung, die Berichterstellung und die Benachrichtigung. Notification Server hostet die webbasierte Management-Konsole, mit der Sie die Komponenten Ihrer Symantec Management-Plattform verwalten können.

Siehe "Komponenten der Symantec Management-Plattform" auf Seite 27.

Siehe "Info zum Konfigurieren von Notification Server" auf Seite 67.

Notification Server ist für das Verwalten der vordefinierten Richtlinien und der Aufgaben verantwortlich, die mit jeder installierten Lösung verfügbar sind. Diese

Richtlinien und Aufgaben aktivieren Komponenten des Notification Servers, die ihrerseits mehrere Funktionen verarbeiten.

Notification Server-Funktionen:

- Ressourcen im Netzwerk erkennen
- Management Agent auf den Endpunkten installieren und konfigurieren
- Durch den Client gemeldete Informationen sammeln und in der CMDB speichern
- Ausführliche Internet-Berichte generieren
- Richtlinieninformationen zu den Endpunkten senden
- Softwarepakete verteilen

Info zum Konfigurieren von Notification Server

Die standardmäßigen Notification Server-Konfigurationseinstellungen sind für die meisten Zwecke geeignet und müssen normalerweise nicht geändert werden. Diese Standardeinstellungen werden festgelegt, wenn Sie die Symantec Management-Plattform installieren. Da sich jedoch die Anforderungen Ihrer Organisation ändern, können Sie die entsprechenden Konfigurationsänderungen vornehmen.

Siehe "Informationen zum Notification Server" auf Seite 66.

Tabelle 3-1 Konfigurationstypen

Konfiguration	Beschreibung
Konfigurieren der Configuration Management Database (CMDB)-Einstellungen	Siehe "Konfigurieren von Configuration Management Database" auf Seite 78.
Einrichten der Datenbankbereinigung	Siehe "Bereinigen der Configuration Management Database" auf Seite 82.
Konfigurieren der Aufbewahrung des Ressourcendatenverlaufs	Siehe "Speichern des Ressourcendatenverlaufs in der CMDB" auf Seite 84.
Konfigurieren der Notification Server-Einstellungen. Diese Einstellungen umfassen Ereignisverarbeitung, Statusmeldungsprotokollierung, E-Mail-Server und Standardadressen sowie einen Proxyserver.	Siehe "Konfigurieren von Notification Server-Einstellungen" auf Seite 68.

Konfiguration	Beschreibung
Konfigurieren der Notification Server-Einstellungen, die nicht in der Symantec Management Console erscheinen	Siehe "Konfigurieren von Notification Server-Einstellungen mit NS Configurator" auf Seite 77.
Angeben der Identifikationsdaten des Verteilungspunkts für Software Delivery-Pakete	Siehe "Einstellungen für Verteilungspunkt-Identifikationsdaten" auf Seite 76.

Konfigurieren von Notification Server-Einstellungen

Zu den konfigurierbaren Notification Server-Einstellungen gehören die Ereignisverarbeitung, die Protokollierung von Statusmeldungen, der E-Mail-Server und dessen Standardadressen.

Siehe "Info zum Konfigurieren von Notification Server" auf Seite 67.

Sie können auch andere Notification Server-Einstellungen mit NS Configurator konfigurieren.

Siehe "Konfigurieren von Notification Server-Einstellungen mit NS Configurator" auf Seite 77.

So konfigurieren Sie Notification Server-Einstellungen

1. Klicken Sie in "Symantec Management Console" im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster unter "Einstellungen" den Ordner "Notification Server" und klicken Sie dann auf "Notification Server-Einstellungen".

3 Nehmen Sie auf der Seite "Notification Server-Einstellungen" die entsprechenden Änderungen auf den folgenden Registerkarten vor:

Verarbeitung	Sie können die Notification Server Event (NSE)-Verarbeitung aktivieren oder deaktivieren, die Anwendungsidentität von Notification Server festlegen und Notification Server-Dienste manuell neu starten. Siehe "Notification Server-Verarbeitungseinstellungen" auf Seite 69.
E-Mail	Sie können den von Notification Server verwendeten Mail-Server angeben und die Standard-E-Mail-Adressen für "An:" und "Von:" festlegen. Siehe "Einstellungen für E-Mail-Server und -Adresse" auf Seite 73.
Protokollieren	Sie können angeben, welche Art von Statusmeldung Notification Server aufzeichnet (Notification Server-Fehler, Warnungen, Informationsmeldungen etc.). Siehe "Einstellungen für die Protokollierung von Statusmeldungen" auf Seite 74.
Proxy	Wenn Notification Server-Benutzern der direkte Zugang zum Netzwerk nicht gestattet werden soll, können Sie einen Proxy-Server konfigurieren. Siehe "Proxy-Server-Einstellungen" auf Seite 75.
Verteilungspunkt-Identifikationsdaten	Sie können die von Notification Server für den Zugriff auf Ihre Paketverteilungspunkte verwendeten Identifikationsdaten angeben. Siehe "Einstellungen für Verteilungspunkt-Identifikationsdaten" auf Seite 76.

4 Klicken Sie auf "OK".

Notification Server-Verarbeitungseinstellungen

Auf der Registerkarte "Verarbeitung" können Sie die Notification Server-Ereignis(NSE)-Verarbeitung aktivieren oder deaktivieren und die Anwendungsidentität von Notification Server angeben Ein NSE ist eine XML-Datei, die vom Notification Server an den Symantec Management-Agent (und Solution-Plugins) weitergeleitet wird.

Auf dieser Registerkarte können Sie auch die Legacy-Agent-Kommunikation konfigurieren.

Siehe "Konfigurieren von Notification Server-Einstellungen" auf Seite 68.

Tabelle 3-2 Optionen auf der Registerkarte "Verarbeitung" Registerkarte

Option	Beschreibung
Server-Verarbeitung	Die Verarbeitung der Notification Server-Ereignisse wird bei der Installation von Notification Server standardmäßig aktiviert. In bestimmten Situationen kann es jedoch erforderlich sein, diese Funktion zu deaktivieren oder wieder zu aktivieren. So wird beispielsweise bei der Installation einer Lösung die gesamte Ereignisautomatisierung automatisch vorübergehend gestoppt. Nach Abschluss der Installation wird die Ereignisverarbeitung normalerweise automatisch fortgesetzt. Ist dies nicht der Fall, wird in der Symantec Management Console eine Warnmeldung angezeigt, in der Sie aufgefordert werden, die NSE-Verarbeitung manuell zu reaktivieren. Klicken Sie zum Reaktivieren der NSE-Verarbeitung zuerst auf die Warnmeldung und dann in dem anschließend geöffneten Dialogfeld auf "Fortsetzen". Die NSEs, die eingehen, während die NSE-Verarbeitung deaktiviert ist, werden auf dem Notification Server-Computer gespeichert und verarbeitet, wenn die NSE-Verarbeitung wieder aktiviert wird. NSEs enthalten z. B. folgende Informationen: ■ Kommunikation mit dem Symantec Management-Agent ■ Ereignisverarbeitung ■ Grundinventar oder vollständiges Inventar ■ Erfolgreicher oder fehlgeschlagener Paket-Download

Option	Beschreibung
Anwendungsidentität	

Option	Beschreibung
	Die Anwendungsidentität von Notification Server ist das Konto, unter dem Notification Server ausgeführt wird. Sie geben den erforderlichen Benutzernamen und das erforderliche Kennwort während der Notification Server-Installation an; im Allgemeinen müssen Sie diese Angaben nur aktualisieren, wenn dies aufgrund von Richtlinien erforderlich wird. Wenn Ihr Unternehmen beispielsweise eine Richtlinie für Kennwortänderungen definiert hat, wird die Änderung der Identifikationsdaten für den CMDB-Zugriff möglicherweise erzwungen. Die Anwendungsidentität ist nicht mehr autorisiert, sich am SQL Server anzumelden. **Warnung:** Sie dürfen keine Sonderzeichen im Benutzernamen oder Kennwort der Anwendungsidentität verwenden. Sie dürfen nur alphanumerische Zeichen verwenden. Die von Ihnen definierte Benutzer-ID erfordert die folgenden Berechtigungen: ■ Lokale Administratorrechte für Notification Server und für alle Remote-Computer mit Windows 2000/XP/2003/Vista, auf denen Sie den Symantec Management-Agent installieren möchten. ■ Die Berechtigung zum Handeln als Teil des Betriebssystems und zur Anmeldung als Stapelverarbeitungsauftrag und Service. ■ Die Berechtigung zur Anmeldung am SQL Server. Wenn die Benutzer-ID nicht über diese Berechtigung verfügt, können Sie einen anderen Benutzernamen und ein anderes Kennwort zur Anmeldung an der CMDB angeben. ■ Die Berechtigung, mit jedem SQL Server eine Verbindung herzustellen, mit dem Notification Server verbunden wird. Beispiele: Eine SMS-Datenbank für "Web Administrator für SMS" oder eine Lease-Datenbank für Contract Management Solution. Notification Server-Dienste werden automatisch neu gestartet, wenn die Anwendungsidentität geändert wird. Mit der Option "Dienste neu starten" können Sie die Dienste nach Bedarf manuell neu starten. Wenn Sie beispielsweise eine Änderung an der Datenbank vornehmen, müssen Sie die Dienste neu starten, damit die Änderungen wirksam werden.

Option	Beschreibung
	Wenn das Kennwort für die Anwendungsidentität fehlschlägt, kann Notification Server nicht auf die CMDB zugreifen. Sie können die Anwendungsidentität nicht über die Symantec Management Console zurücksetzen, da die Konsole dasselbe Kennwort für den Zugriff auf Notification Server verwendet. Sie müssen stattdessen mit dem Dienstprogramm "ASConfig" direkt auf die Web Services zugreifen und das Kennwort für die Anwendungsidentität mit der relevanten Befehlszeile zurücksetzen.
Legacy-Agent-Kommunikation	Hier können Sie festlegen, ob die Endgeräte, die ältere Versionen von Symantec Management Agent verwenden, mit mit dem aktualisierten Notification Server kommunizieren können. Ist der Modus "Legacy-Agent-Kommunikation" aktiviert (LAC) deaktiviert, können Sie nur aktualisierten Agents aktiv verwalten. Ist der Modus "LAC" aktiviert, können Sie einen begrenzten Satz Verwaltungsaufgaben auf den Legacy-Agents ausführen. Siehe "Informationen zur Legacy-Agent-Kommunikation" auf Seite 284.

Einstellungen für E-Mail-Server und -Adresse

Sie können einen Mail-Server und die "An:"- und "Von:"-E-Mail-Adressen für Notification Server-E-Mail-Nachrichten definieren. Notification Server verwendet zum Senden von E-Mail-Nachrichten das SMTP-Protokoll. Die E-Mail-Adresse kann eine gültige SMTP-Adresse sein, die von Ihrem SMTP-Server erkannt wird.

Siehe "Konfigurieren von Notification Server-Einstellungen" auf Seite 68.

Sie können festlegen, dass Symantec-Lösungen Ihnen E-Mails senden, die auf Daten basieren, die der Notification Server empfängt. Die von Ihnen angegebene E-Mail-Adresse kann Benachrichtigungen über erfolgreich ausgeführte Berichte, abgeschlossene Automatisierungsaktionen und Systemskalierbarkeitsprüfungen empfangen. Diese E-Mails unterstützen Sie bei der Überwachung und Verwaltung Ihrer Notification Server-Aktivitäten

Die E-Mail-Einstellungen werden konfiguriert, wenn Sie Notification Server installieren. Sie müssen normalerweise nicht von Ihnen geändert werden. Wenn sich der SMTP-Server jedoch ändert oder Sie veranlassen möchten, dass die E-Mail-Nachrichten an einen anderen Empfänger gesendet werden, müssen Sie die Einstellungen entsprechend ändern.

Über die Option "Test-E-Mail senden" können Sie die E-Mail-Server- und Adresseinstellungen testen, indem Sie eine E-Mail unter Verwendung der aktuellen Einstellungen senden. Die Änderungen müssen durch Klicken auf "OK" vor dem Senden der Test-E-Mail bestätigt werden.

Einstellungen für die Protokollierung von Statusmeldungen

Sie können angeben, welche Art von Statusmeldung Notification Server aufzeichnen soll (Notification Server-Fehler, Warnungen, Informationsmeldungen etc.). Standardmäßig werden die Protokollmeldungen, die Notification Server erzeugt, in Protokolldateien im Ordner `...\Programme\Altiris\Notification Server\Logs` geschrieben.

Hinweis: Wenn Notification Server von 6.x auf 7.x aktualisiert wird, schreibt der Migrationsassistent alle Meldungen in die Protokolldatei von Version 6.x und nicht in die von 7.0. Der Speicherort der Protokolldatei von Version 6.x ist `...\Programme\Altiris\Notification Server\Logs`. Sie müssen diese Protokolldatei anzeigen, um Migrationsfehler zu überprüfen. Die Protokollanzeige zeigt nur die Protokolle an, die im 7.0-Standardverzeichnis archiviert sind. Die Migrationsprotokolleinträge sind nicht enthalten.

Siehe "Konfigurieren von Notification Server-Einstellungen" auf Seite 68.

Folgende Meldungen können protokolliert werden:

- Fehler
- Warnungen
- Informationen
- Verfolgung
- Ausführlich

Sie können auch veranlassen, dass Protokolldateien nach einer bestimmten Zeitspanne archiviert werden. Wenn Sie diese Option aktivieren, werden die relevanten Protokolldateien täglich um 5:00 Uhr archiviert.

Siehe "Öffnen der Protokollanzeige" auf Seite 74.

Öffnen der Protokollanzeige

Mit der Protokollanzeige können Sie mehrere Speicherorte für Protokolle auf verschiedene Komponenten wie IT Management Suite, Symantec Management-Agent und Symantec Installation Manager überwachen. Die Protokollanzeige erkennt automatisch, ob eine Komponente in einem

benutzerdefinierten Speicherort installiert ist und überwacht den benutzerdefinierten Pfad. Die Protokollanzeige listet die Echtzeitereignisse, Fehler und Warnungen auf, die auftreten, wenn eine beliebige Aktion ausgeführt wird. Diese Meldungen helfen Ihnen bei der Überwachung des und der Fehlerbehebung auf dem Notification Server.

Mit der Protokollanzeige können Sie Probleme und deren Ursache ermitteln. Nachdem Sie Fehler oder Warnungen in der Protokollanzeige identifiziert haben, können Sie anhand der Fehlermeldungen die Symantec-Supportdatenbank nach Artikeln durchsuchen, die Ihnen beim Beheben des Fehlers helfen können. Sie können das Problem auch dem technischen Support melden.

In der Protokollanzeige haben Sie folgende Möglichkeiten:

- Anzeigen von Fehler-, Warn-, Informations-, Trace- und ausführlichen Meldungen
- Durchsuchen der Protokolle und Anzeigen der Ergebnisse
- Erstellen von Lesezeichen für Protokollelemente
- Filtern der Protokolle zum Anzeige einer Teilmenge der Meldungen
- Speichern der Filterdefinitionen für die spätere Verwendung
- Durchsuchen von Protokolldateien ohne sie in die Protokollanzeige laden zu müssen

Siehe "Einstellungen für die Protokollierung von Statusmeldungen" auf Seite 74.

Version 7.5 von IT Management Suite führt eine neue Protokollanzeige mit erweiterten Funktionen und bessere Benutzerfreundlichkeit ein. Beachten Sie, dass Sie auch die ältere Altiris-Protokollanzeige verwenden können, die zu Kompatibilitätszwecken im Produkt verbleibt und "Legacy-Protokollanzeige" genannt wird.

So öffnen Sie die neue Protokollanzeige

- Klicken Sie auf dem Notification Server-Computer auf "Start" und wählen Sie "Alle Programme > Symantec > Diagnostics > Altiris Log Viewer".

So öffnen Sie die Legacy-Protokollanzeige

- Klicken Sie auf dem Notification Server-Computer auf "Start" und wählen Sie "Alle Programme > Symantec > Diagnostics > Altiris Legacy Log Viewer".

Proxy-Server-Einstellungen

Wenn Notification Server-Benutzern der direkte Zugang zum Netzwerk nicht gestattet werden soll, können Sie einen Proxy-Server konfigurieren. Beispielsweise bei Notification Server und verwalteten Computer innerhalb der Firewall einer Organisation kann ein Proxy-Server Sicherheit zusätzliche Sicherheit bieten. Sie

können einen Proxy-Server einrichten, um eine sicheren Weg durch die Firewall ohne Risiko für den Notification Server zur Verfügung zu stellen. Damit helfen Sie Notification Server, Patches oder Download-Lösungen sicher von externen Websites zu laden.

Siehe "Konfigurieren von Notification Server-Einstellungen" auf Seite 68.

Die Verwendung eines Proxy-Servers kann die Notification Server-Leistung verbessern, da das Anfordern von Dateien aus dem Internet weniger Bandbreite und weniger Filteranfragen erfordert. Ein Beispiel sind PMImport-Daten.

Die Option "Einstellungen testen" überprüft die Proxy-Server-Einstellungen, indem versucht wird, eine Verbindung mit einer externen Website herzustellen.

Wenn beim Testen der Einstellungen Fehlermeldungen angezeigt werden, stellen Sie sicher, dass Ihre Authentifizierungsdaten richtig sind. Stellen Sie sicher, dass Ihr Proxy-Server ausgeführt wird und keine allgemeinen Netzwerkfehler vorliegen.

Einstellungen für Verteilungspunkt-Identifikationsdaten

Sie können festlegen, welche Verteilungspunkt-Identifikationsdaten (Distribution Point Credentials, DPC) Notification Server für den Zugriff auf Software Delivery-Paket verwendet. Die Software Delivery-Pakete befinden sich in einer Netzwerkfreigabe, auf die über einen UNC-Pfad Zugriff besteht. Notification Server veröffentlicht diese Pakete in einem virtuellen HTTP-Verzeichnis, das über DPC mit der UNC-Freigabe verbunden wird.

Siehe "Konfigurieren von Notification Server-Einstellungen" auf Seite 68.

Sie müssen die Verteilungspunkt-Identifikationsdaten angeben, bevor Sie ein Softwarepaket erstellen, auf das von einem vorhandenen UNC-Pfad aus zugegriffen wird. Die Identifikationsdaten müssen berechtigt sein, Benutzerkonten zu überprüfen, und sie müssen über Leseberechtigung für alle Dateien auf den Remote-Verteilungspunkten verfügen.

Notification Server unterstützt alle im Folgenden aufgeführten Identifikationsdaten:

Agent-Authentifizierungsinformationen	Alle Symantec Management-Agents verwenden ACC (Agent Connectivity Credential) zum Herstellen einer Verbindung zu einer sicheren Ressource. ACC wird in der Richtlinie "Globale Agent-Einstellungen" festgelegt.

Vom Benutzer angegebene Identifikationsdaten	Wenn die Pakete an einem Ort gespeichert werden, der nicht mit den Agent-Identifizierungsinformationen zugänglich ist, können Sie sie zugänglich machen. Geben Sie den Benutzernamen und das Kennwort eines Kontos mit entsprechendem Zugriff an, um Pakete zugänglich zu machen. Sie können keine Sonderzeichen im Benutzernamen oder Kennwort verwenden. Sie dürfen nur alphanumerische Zeichen verwenden.

Konfigurieren von Notification Server-Einstellungen mit NS Configurator

NS Configurator ist ein Konfigurationstool, mit dem Sie die meisten zentralen Konfigurationseinstellungen des Notification Servers ändern können. Viele dieser Einstellungen sind nicht von der Symantec Management Console aus zugänglich. Sie sollten NS Configurator nur verwenden, wenn Sie wissen, welche Auswirkung die Einstellungen auf das System haben.

Siehe "Info zum Konfigurieren von Notification Server" auf Seite 67.

Nach dem Aufrufen von NS Configurator wird eine Sicherheitsprüfung durchgeführt, um zu bestimmen, ob der Benutzer zum Anzeigen bzw. Ändern der Notification Server-Einstellungen berechtigt ist. Ist dies nicht der Fall, wird eine Warnmeldung ausgegeben und das Tool wird beendet.

So konfigurieren Sie Notification Server-Einstellungen mit NS Configurator

1. Führen Sie die Datei "NSConfigurator.exe" aus.

   Sie befindet sich unter "Programme\Altiris\Notification Server\Bin\Tools". Wenn Sie dieses Tool ausführen, öffnet es die Datei "CoreSettings.config", die sich unter "Programme\Altiris\Notification Server\Config" befindet.

2. Sie haben folgende Möglichkeiten zum Suchen der zu ändernden Einstellungen:

   - Suchen Sie die Einstellung in der Verzeichnisstruktur im linken Teilfenster.
   - Geben Sie im Suchfeld oben rechts den Suchbegriff ein und klicken Sie auf "Suchen". Klicken Sie in der Liste der Suchergebnisse neben der gewünschten Einstellung auf "Anzeigen".

3 Ändern Sie die Einstellung im rechten Teilfenster und klicken Sie auf "Speichern".

   Wenn Sie einen ungültigen Wert für eine Einstellung eingeben, wird eine Fehlermeldung ausgegeben. Sie können die Änderungen nur speichern, wenn Sie einen gültigen Wert eingeben.

4 Klicken Sie zum Wiederherstellen des Standardwerts auf "Standard wiederherstellen".

   Die Option "Standard wiederherstellen" wird nur angezeigt, wenn die Einstellung einen Standardwert hatte.

Konfigurieren von Configuration Management Database

Notification Server hat eine Datenbank, die sog. Configuration Management Database (CMDB). Notification Server und -Lösungen nutzen die CMDB zum Speichern von Konfigurationselementen und Ressourcendaten.

Die Verarbeitung der Datenbank ist einer der größten Ressourcenverbraucher in Symantec Management Platform. Die Anzahl von Lösungen, die in Ihrer Umgebung installiert sind, und ihre Verwendung beeinflusst die Anforderungen der Datenbank. Die Anzahl der verwalteten Computer, die jedem Notification Server-Computer berichten, beeinflusst die Datenbankanforderungen ebenfalls.

Jeder Notification Server-Computer kann so konfiguriert werden, dass er eine lokale Configuration Management Database (CMDB) oder die Remote-CMDB verwendet. Ein Notification Server-Computer mit einer lokalen Datenbank erfordert mehr Ressourcen als ein Notification Server-Computer mit einer Remote-Datenbankkonfiguration.

Sie können die folgenden Konfigurationen für die CMDB verwenden:

Lokale CMDB-Konfiguration	In einer lokalen CMDB-Serverkonfiguration wird CMDB auf demselben Computer wie Notification Server installiert. Diese Konfiguration ist für die Umgebungen mit 1.000 bis 5.000 Endgeräte akzeptabel. In diesen Umgebungen gibt es zwischen den Notification Server-Diensten und den CMDB-Diensten minimalen Wettstreit um Ressourcen.

Remote-CMDB-Konfiguration	In einer Remote-CMDB-Konfiguration installieren Sie CMDB auf einem anderen Computer als dem Notification Server-Computer. Diese Konfiguration wird für die meisten Umgebungen empfohlen. In dieser Konfiguration wird der Notification Server-Computer von der Arbeitslast der CMDBs entlastet. Zwischen CMDB-Server und Notification Server-Computer muss eine Hochgeschwindigkeitsnetzwerkverbindung bestehen. Symantec empfiehlt 1-Gbit-Ethernet.

Sie können alle notwendigen Änderungen an den CMDB-Konfigurationseinstellungen vornehmen. Wenn Notification Server installiert wird, wird CMDB als Teil des Installationsprozesses konfiguriert. Sie müssen normalerweise keine weiteren Änderungen vornehmen.

Jedoch kann es vorkommen, dass Sie die CMDB-Konfigurationseinstellungen ändern müssen. Beispiel: Wenn Sie ein Upgrade der Hardware durchführen, auf der Ihr Microsoft SQL Server ausgeführt wird, oder wenn Sie dazu durch den Symantec-Support angewiesen werden.

So konfigurieren Sie die Configuration Management Database

1 Klicken Sie in Symantec Management Console im Menü "Einstellungen" auf "Notification Server" > "Datenbankeinstellungen".

2 Nehmen Sie auf der Seite "Datenbank-Einstellungen" auf den Registerkarten "Allgemein" und "Berichte" die entsprechenden Konfigurationsänderungen vor.

Name des Datenbankservers	Der Name des SQL-Servers, der die CMDB enthält. Verwenden Sie das folgende Format: *Servername\Instanzname*. Beispiel: **SydNS\sql_cp1_cs_as**.
Datenbank-identifikationsdaten	Der Benutzername und das Kennwort, der/das für den Zugriff auf CMDB erforderlich ist. Sie können die Notification Server-Anwendungsidentifikationsdaten zur Windows-Authentifizierung verwenden. Es empfiehlt sich, diese Methode zu verwenden, um nicht von jeder Richtlinie für Kennwortänderung betroffen zu sein, die in Ihrer Organisation durchgesetzt wird. Die Anwendungsidentifikationsdaten werden auf der Seite "Servereinstellungen" auf der Registerkarte "Verarbeitung" angegeben. Siehe "Notification Server-Verarbeitungseinstellungen" auf Seite 69. Sie haben auch die Option, die SQL-Authentifizierung zu verwenden. Sie können auch zum Einsatz der SQL-Authentifizierung den entsprechenden SQL-Benutzernamen und das -Kennwort angeben. **Hinweis:** Wenn Sie aus der Datenbank-Authentifizierung in SQL wechseln möchten, müssen Sie diese Änderung auf beiden Registerkarten ("Allgemein" und "Berichte") vornehmen. Die Registerkarte "Allgemein" ist die Standardregisterkarte, die erscheint, wenn Sie die Seite "Datenbankeinstellungen" öffnen. Wenn Sie die Änderung nur auf der Registerkarte "Allgemein" vornehmen, ist Notification Server nicht voll funktionell und kann in einigen Vorgängen Fehler verursachen.
Datenbankname	Sie können eine vorhandene Datenbank aus der Liste der verfügbaren Datenbanken auswählen oder eine neue Datenbank erstellen. Wenn Sie eine vorhandene Datenbank auswählen, stellen Sie sicher, dass sie die gleiche Version wie Notification Server hat.

Datenbank reparieren	Mit dieser Option können Sie CMDB reparieren. Sie müssen unter Umständen diese Vorgehensweise wählen, wenn Sie Notification Server von einem Backup auf einem neuen Computer wiederherstellen.
Befehls-Timeout	Der Zeitraum, in dem Notification Server versucht, eine Abfrage zu verarbeiten (z. B. das Ausführen eines Berichts oder Aktualisieren eines Filters). Sie sollten diesen Wert ändern, wenn beispielsweise eine hohe Belastung auf dem SQL-Server eine Zeitüberschreitung für Abfragen zur Folge haben kann. Symantec empfiehlt, dass Sie in Microsoft IIS die Option "ASP-Skripttimeout:" auf einen Wert größer oder gleich dem Wert von "Befehls-Timeout" festzulegen. Wenden Sie sich an Ihren Datenbankadministrator, bevor Sie Änderungen vornehmen.
Identifikationsdaten für öffentlichen Bericht	Der Sicherheitskontext, der für die Ausführung von Berichtsabfragen in CMDB verwendet werden soll. Diese Identifikationsdaten bieten weniger Sicherheit als Datenbankberechtigungen (die für den Datenbankadministrator bestimmt sind). Diese Identifikationsdaten werden verwendet, um auf die Datenbank zuzugreifen und die entsprechende SQL-Abfrage auszuführen, wenn ein Benutzer einen Bericht ausführt.

3 Klicken Sie auf "Änderungen speichern".

Siehe "Info zum Konfigurieren von Notification Server" auf Seite 67.

Bereinigen der Configuration Management Database

Um die Größe der Configuration Management Database zu verwalten (CMDB), können Sie angeben, wie lange bestimmte Typen von Daten gespeichert werden. Sie können die Speicherlänge für Daten wie etwa Berichte, verwaltete Computer und Ereignisdaten angeben. Wenn Sie bei der Ausführung Ihrer Berichte feststellen, dass die Leistung der Datenbank zu wünschen übrig lässt, sollten Sie versuchen, Ihre Ereignisse zu bereinigen oder die Optionen für die Ereignisbereinigung so konfigurieren, dass weniger Daten gespeichert werden.

Siehe "Konfigurieren von Configuration Management Database" auf Seite 78.

Es können u.a. folgende Daten aus der CMDB entfernt werden:

- Berichtschnappschüsse

Schnappschüsse, die ein bestimmtes Datum überschritten haben, können gelöscht werden.

- Die verwalteten Computer, die über den angegebenen Zeitraum hinaus nicht mit dem Notification Server kommuniziert haben.
  Diese Daten können gelöscht oder als stillgelegt gekennzeichnet werden. Die CMDB wird während der Ausführung des CMDB-Bereinigungszeitplans aktualisiert.
- Ressourcenereignisdaten
  Ereignisdaten, die länger als eine angegebene Zeitspanne gespeichert wurden, können gelöscht werden. Optional können Sie festlegen, wie viele Reihen maximal zurückbehalten werden sollen. Wenn die Ereignisdatentabelle die angegebene Größe erreicht, werden bis zur nächsten zeitplangesteuerten Aktualisierung neue Reihen hinzugefügt. Wenn der CMDB-Bereinigungszeitplan ausgeführt wird, wird die Tabelle auf ihre maximale Größe getrimmt. Die Tabelle wird getrimmt, indem die ältesten Zeilen entfernt werden, selbst wenn die ältesten Daten nicht für die angegebene Zeit beibehalten wurden.
  Sie können dieselben Einstellungen für alle Datenklassen verwenden oder benutzerdefinierte Einstellungen für einzelne oder alle Datenklassen festlegen. Eine benutzerdefinierte Einstellung für eine Datenklasse setzt die globale Einstellung außer Kraft. Wenn keine benutzerdefinierte Einstellung für eine Datenklasse definiert ist, wird die globale Einstellung für die betreffende Datenklasse verwendet. In allen Fällen wird derselbe CMDB-Bereinigungszeitplan verwendet.

Der CMDB-Bereinigungszeitplan ist ein Windows-Zeitplan, der beim Installieren von Notification Server konfiguriert wird. Er kann nicht über die Symantec Management Console geändert werden. Änderungen können nach Bedarf über die Systemsteuerung in Windows vorgenommen werden.

So bereinigen Sie die Configuration Management Database

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server" > "Bereinigungseinstellungen".
2. Klicken Sie im linken Teilfenster unter "Bereinigungseinstellungen" auf "Bereinigungseinstellungen".

3 Konfigurieren Sie auf der Seite "Bereinigungseinstellungen" die Einstellungen auf den folgenden Registerkarten:

Bereinigungseinstellungen	Geben Sie hier die Bereinigungseinstellungen für Berichte, Agent-Registrierungsdaten und Computerdaten an. Beachten Sie, dass die Option "Veraltete Agent-Registrierungseinträge bereinigen" nur Elemente mit dem Status "Blockiert" löscht. Zum Übergehen des Bereinigungszeitplans und sofortigen Bereinigen der CMDB klicken Sie auf "Jetzt bereinigen".
Bereinigungseinstellungen für Ressourcenereignis-Daten	Geben Sie hier die gewünschten Bereinigungseinstellungen für Ressourcenereignis-Daten an.
Einstellungen für Bereinigung von Berichtsdaten-Snapshots	Geben Sie hier die Einstellungen für Bereinigung von Berichtsdaten-Snapshots an. Zum Übergehen des Bereinigungszeitplans und sofortigen Bereinigen der CMDB klicken Sie auf "Jetzt bereinigen".

4 Klicken Sie auf "Änderungen speichern".

Speichern des Ressourcendatenverlaufs in der CMDB

Notification Server speichert Ressourcendaten in Echtzeit im Rahmen des Inventarisierungsvorgangs. Der Ressourcendatenverlauf kann für jede Art von Ressource und jede Ressourcenzuordnung erstellt werden. Für jeden Verlauf können Sie angeben, wie lange die Verlaufsdaten in der CMDB beibehalten werden sollen.

Siehe "Konfigurieren von Configuration Management Database" auf Seite 78.

Ein Ressourcendatenverlauf kann Daten aus allen Datenklassen einschließen. Ein Ressourcendatenverlauf kann Daten eines jeden Ressourcenzuordnungstyps beinhalten.

So speichern Sie den Ressourcendatenverlauf in der CMDB

1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Bereinigungseinstellungen".

2 Klicken Sie im linken Teilfenster im Ordner "Bereinigungseinstellungen" auf "Ressourcenverlauf".

3 Gehen Sie auf der Seite "Ressourcenverlauf" für jeden Ressourcendatenklassentyp und jede Ressourcenzuordnung, die Sie konfigurieren möchten, auf den entsprechenden Registerkarten wie folgt vor:

- Erweitern Sie die Datenklasse oder den Zuordnungstyp.
- Wählen Sie die Datenklassen oder Zuordnungen aus, für die Sie den Ressourcendatenverlauf erstellen möchten.
- Geben Sie für jede Datenklasse oder Zuordnung an, wie lange der Ressourcendatenverlauf gespeichert werden soll.
  In der entsprechenden Dropdown-Liste wählen Sie den Zeitraum aus (Tage, Wochen oder Monate). Geben Sie die entsprechende Anzahl der Tage, Wochen oder Monate ein.

Alle Ressourcendaten, die älter sind als das für den jeweiligen Typ festgelegte zeitliche Maximum, werden während des zeitplangesteuerten Bereinigungsvorgangs aus der CMDB gelöscht.

4 Klicken Sie auf "Änderungen speichern".

Kapitel 4

Konfigurieren der Sicherheit

In diesem Kapitel werden folgende Themen behandelt:

- Infos zur Sicherheit der Symantec Management-Plattform
- Einrichten der Sicherheit für die Symantec Management-Plattform
- Sicherheitsverwaltungsaufgaben für Symantec Management-Plattform

Infos zur Sicherheit der Symantec Management-Plattform

Die Symantec Management-Plattform verwendet rollenbasierte Sicherheit, d. h., der Benutzerzugriff basiert auf der dem jeweiligen Benutzer zugewiesenen Sicherheitsrolle. Eine Sicherheitsrolle ist ein Satz von Privilegien und Berechtigungen, der allen Mitgliedern dieser Rolle zugewiesen wird. Mithilfe der rollenbasierten Sicherheit können Sie eine geringe Anzahl von Sicherheitsrollen erstellen und verwalten. Sie können dann jedes Symantec Management-Plattform-Benutzerkonto der entsprechenden Rolle zuweisen, statt jedem einzelnen Benutzer bestimmte Privilegien und Berechtigungen zuweisen zu müssen. Sie können jedoch auch einzelnen Benutzerkonten bestimmte Berechtigungen zuweisen.

Benutzerkonten, auch als Benutzer bezeichnet, sind nicht dasselbe wie Benutzerressourcen in der Symantec Management-Plattform. Eine Benutzerressource ist eine Entität, die verwendet wird, um verwaltete Geräte mit dem Besitzer des Geräts zu verknüpfen. Die vorhandenen Benutzerressourcen und die Benutzerkonten, die bei der Symantec Management Console einloggen oder einen Workflow ausführen können, sind separate Entitäten.

Eine Sicherheitsrolle regelt den Benutzerzugriff auf die Symantec Management-Plattform auf folgende Weise:

- Privilegien
  Ein Recht gilt systemweit. Privilegien werden nur Rollen zugewiesen und können nicht direkt einzelnen Benutzerkonten zugewiesen werden. Ein Recht, das einer Rolle zugewiesen wird, ermöglicht einem Benutzerkonto, das Mitglied dieser Rolle ist, das Ausführen einer bestimmten Aktion auf der Symantec Management-Plattform oder in der Symantec Management Console. In einigen Fällen erfordert die Rolle des Benutzers entsprechende Berechtigungen.
  Siehe "Sicherheitsprivilegkategorien" auf Seite 510.
- Berechtigungen für Ordner und Elemente
  Berechtigungen geben den Zugriff an, den eine Sicherheitsrolle oder ein Benutzerkonto auf einen Ordner oder ein Element der Symantec Management Console hat. Eine Berechtigung für eine Sicherheitsrolle gilt für alle Mitglieder dieser Rolle. Die Berechtigung für einen Ordner gilt für alle direkt in dem Ordner enthaltenen Elemente.
  Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.
- Berechtigungen für Organisationsübersichten und Gruppen
  Eine Organisationsansicht ist eine hierarchische Ressourcengruppe (genau wie Organisationsgruppen), die einer tatsächlichen Struktur oder Übersicht Ihres Unternehmens entspricht. Sie können Ressourcensicherheit einrichten, indem Sie jeder Sicherheitsrolle die entsprechenden Berechtigungen für die einzelnen Organisationsansichten zuweisen. Außerdem können Sie die entsprechenden Berechtigungen für die Organisationsgruppen innerhalb jeder Ansicht zuweisen. Eine Berechtigung, die einer Organisationsgruppe zugewiesen wird, gilt für alle Ressourcen in dieser Gruppe. Standardmäßig gilt diese Berechtigung auch für alle untergeordneten Gruppen. Sie können Berechtigungen nicht direkt einer bestimmten Ressource zuweisen.

Privilegien, Berechtigungen für Ordner und Elemente und Berechtigungen für Organisationsansichten und Gruppen funktionieren im Einklang miteinander. Sie müssen jeder Sicherheitsrolle die richtige Kombination zuordnen, damit die Benutzerkonten den benötigten Zugriff zur Ausführung der vorgesehenen Aktivitäten haben.

Siehe "Einrichten der Sicherheit für die Symantec Management-Plattform" auf Seite 88.

Siehe "Sicherheitsverwaltungsaufgaben für Symantec Management-Plattform" auf Seite 114.

Einrichten der Sicherheit für die Symantec Management-Plattform

Um Benutzerkonten Zugriff auf die Symantec Management-Plattform, installierte Lösungen und die Daten in der CMDB zu gewähren, müssen Sie die Sicherheitsrollen einrichten. Sie weisen jeder Rolle die entsprechenden Privilegien und Berechtigungen zu. Sie müssen Symantec Management-Plattform-Benutzerkonten erstellen und anschließend jedes Benutzerkonto der entsprechenden Rolle (bzw. den Rollen) zuweisen.

Siehe "Infos zur Sicherheit der Symantec Management-Plattform" auf Seite 86.

Tabelle 4-1 Einrichten der Sicherheit der Symantec Management-Plattform

Schritt	Aktion	Beschreibung
Schritt 1	Erstellen und konfigurieren Sie die erforderlichen Sicherheitsrollen.	Sicherheitsrollen steuern den Zugriff auf die Symantec Management-Plattform, installierte Lösungen und alle Daten, die in der CMDB enthalten sind. Zum Erstellen neuer Sicherheitsrollen haben Sie folgende Möglichkeiten: ■ Erstellen Sie neue Sicherheitsrollen. ■ Duplizieren Sie vorhandene Sicherheitsrollen. ■ Importieren Sie Domänengruppen und Benutzer aus dem Active Directory. Siehe "Erstellen und Konfigurieren von Sicherheitsrollen" auf Seite 91.
Schritt 2	Weisen Sie den Sicherheitsrollen die gewünschten Privilegien zu.	Ein Recht ermöglicht einem Rollenmitglied die Ausführung einer bestimmten Aktion auf der Symantec Management-Plattform oder an Elementen in der Symantec Management Console. Um eine Aktion an einem Element ausführen zu können, muss die Rolle die notwendige Berechtigung für das Element haben. Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Schritt	Aktion	Beschreibung
Schritt 3	Erstellen und konfigurieren Sie die erforderlichen Benutzerkonten.	Jedes Symantec Management-Plattform-Benutzerkonto enthält die Identifikationsdaten, die der Benutzer benötigt, um auf die Symantec Management Console zuzugreifen oder einen Workflow auszuführen. Die Identifikationsdaten können interne Benutzernamen und Kennwörter der Symantec Management-Plattform oder Windows-Konten sein. Interne Identifikationsdaten werden derzeit nur für die Workflow-Integration verwendet. Windows-Identifikationsdaten sind erforderlich, um auf die Symantec Management Console zuzugreifen. Zum Erstellen neuer Benutzerkonten haben Sie folgende Möglichkeiten : ■ Erstellen Sie vollständig neue Benutzerkonten. ■ Duplizieren Sie vorhandene Benutzerkonten. ■ Importieren Sie Domänengruppen und Benutzer aus dem Active Directory. Siehe "Erstellen und Konfigurieren von Benutzerkonten der Symantec Management-Plattform" auf Seite 233. Siehe "Angeben allgemeiner Details für ein Symantec Management-Plattform-Benutzerkonto" auf Seite 101. Siehe "Konfigurieren von Identifikationsdaten für ein Symantec Management-Plattform-Benutzerkonto" auf Seite 102.
Schritt 4	Weisen Sie den entsprechenden Sicherheitsrollen Mitglieder zu.	Ein Benutzer erhält durch seine Mitgliedschaft in einer Sicherheitsrolle Zugriff auf die Symantec Management-Plattform, installierte Lösungen und alle Daten, die in der CMDB enthalten sind. Sie können einen Benutzer einer beliebigen Anzahl von Sicherheitsrollen zuweisen. Ein Benutzer, der Mitglied mehrerer Sicherheitsrollen ist, verfügt über die Kombination aller Privilegien und Berechtigungen, die diese Rollen gewähren. Siehe "Hinzufügen von Mitgliedern für eine Sicherheitsrolle" auf Seite 105. Siehe "Zuweisen eines Symantec Management-Plattform-Benutzerkontos zu einer Sicherheitsrolle" auf Seite 106. Siehe "Hinzufügen von Sicherheitsrollen als Mitglieder anderer Sicherheitsrollen" auf Seite 107.

Schritt	Aktion	Beschreibung
Schritt 5	Weisen Sie jeder Sicherheitsrolle Berechtigungen für die Ordner und Elemente zu, die in der Symantec Management Console enthalten sind.	Berechtigungen geben den Zugriff an, den jede Sicherheitsrolle auf einen Ordner der Symantec Management Console oder auf ein bestimmtes Element hat. Eine Berechtigung für ein Element gilt nur für das betreffende Element. Die Berechtigung für einen Ordner gilt für alle direkt in dem Ordner enthaltenen Elemente. Standardmäßig erben die Inhalte eines Ordners alle Berechtigungen des Ordners. Siehe "Zuweisen von Sicherheitsberechtigungen zu Ordnern und Elementen" auf Seite 108.
Schritt 6	Optional können Sie die Berechtigungsvererbung in der Symantec Management Console-Ordnerstruktur für jede Sicherheitsrolle modifizieren.	Durch Ändern der Berechtigungsvererbung können Sie die Berechtigungen für die Symantec Management Console-Ordnerstruktur anpassen. Sie können also einem übergeordneten Ordner eine bestimmte Berechtigung gewähren und diese Berechtigung aus einigen oder allen Ordnerinhalten entfernen. Denken Sie daran, Berechtigungen für Ordner und die Elemente in den Ordnern zu konfigurieren. Wenn Sie einen Ordner konfigurieren und Schreibberechtigungen für eine bestimmte Rolle bewilligen, hat diese Rolle die Schreibberechtigung für den Ordner und dessen gesamten Inhalt. Wenn der Ordner 100 Elemente enthält und diese Elemente nicht die Schreibberechtigung vom übergeordneten Ordner erben sollen, können Sie die Berechtigungsvererbung aufgliedern. In diesem Fall verfügen Benutzer, die Mitglieder der Rolle sind, der Sie die Schreibberechtigung gewährt haben, über die Schreibberechtigung nur auf den Ordner. Sie verfügen jedoch nicht über Schreibberechtigung auf die Elemente, die der Ordner enthält. Die Berechtigungsvererbung für einen Ordner oder ein Element gilt für alle Sicherheitsrollen. Sie können die Berechtigungsvererbung nicht rollenweise anpassen. Siehe "Anpassen der Vererbungsregeln für Berechtigungen" auf Seite 109.

Schritt	Aktion	Beschreibung
Schritt 7	(Optional) Konfigurieren Sie die Ressourcensicherheit.	Standardmäßig haben alle vordefinierten Sicherheitsrollen die Leseberechtigung auf Ressourcen. Für sicherheitsbezogene Ressourcen gilt eine spezielle Steuerung in der Symantec Management-Plattform: Nur Benutzer, die Mitglieder der Symantec-Administratorrolle sind, haben standardmäßig vollständigen Zugriff auf die Sicherheitsressourcen. Benutzer, die Mitglieder der Rolle für Symantec Vorgesetze sind, haben standardmäßig Leseberechtigung für Sicherheitsressourcen. Keine andere vordefinierte Sicherheitsrolle verfügt über Berechtigungen auf Sicherheitsressourcen. Siehe "Vordefinierte Sicherheitsrollen" auf Seite 112. Wenn Sie den Zugriff auf Ressourcen einschränken oder kontrollieren möchten, müssen Sie die Ressourcensicherheit konfigurieren. Sie konfigurieren die Ressourcensicherheit, indem Sie eine oder mehrere Organisationsansichten erstellen, die Ihre Ressourcenstruktur modellieren. Sie steuern den Zugriff auf die Ressourcen, indem Sie jeder Sicherheitsrolle Berechtigungen für die entsprechenden Organisationsansichten und -gruppen zuweisen.

Erstellen und Konfigurieren von Sicherheitsrollen

Eine Sicherheitsrolle ist ein Satz von Privilegien und Berechtigungen, der allen Mitgliedern dieser Rolle zugewiesen wird. Mithilfe der rollenbasierten Sicherheit können Sie eine geringe Anzahl von Sicherheitsrollen erstellen und verwalten und jedem Benutzerkonto die entsprechende Rolle zuweisen. Sie müssen nicht jedem einzelnen Benutzerkonto Rechte und Berechtigungen zuweisen. Sie können einem Benutzerkonto mehreren Sicherheitsrollen zuweisen: Ein Mitglied mehrerer Sicherheitsrollen verfügt über die Kombination aller Rechte und Berechtigungen, die diese Rollen gewähren.

Siehe "Infos zur Sicherheit der Symantec Management-Plattform" auf Seite 86.

Sicherheitsrollen können verschachtelt werden: Eine Rolle kann Mitglied einer oder mehrerer anderer Rollen sein und ihre Mitgliedschaft kann sowohl Rollen als auch Benutzerkonten umfassen. Die einzige Einschränkung ist, dass Sie keine zirkuläre Rollenmitgliedschaft erstellen können, bei der eine Rolle Mitglied von sich selbst ist.

Privilegien, Berechtigungen für Ordner und Elemente sowie Berechtigungen für Organisationsansichten und Gruppen funktionieren im Einklang miteinander. Sie müssen jeder Sicherheitsrolle die richtige Kombination zuordnen, damit die

Benutzerkonten den benötigten Zugriff zur Ausführung der vorgesehenen Aktivitäten haben. Privilegien können nur Sicherheitsrollen zugewiesen werden, Berechtigungen dagegen Sicherheitsrollen und Benutzerkonten.

Sie müssen bestimmen, welche Sicherheitsrollen Sie basierend auf den logischen Anforderungen für IT-Mitarbeiter und Benutzergruppen Ihrer Organisation erstellen sollten. So können Sie zum Beispiel die Rollen "IT-Mitarbeiter Stufe 1", "Oberes Management" und "Personalabteilung" erstellen. Alle Benutzerkonten in einer Sicherheitsrolle erhalten dieselben Privilegien und Berechtigungen und haben daher denselben Zugriff auf die Symantec Management-Plattform.

Erstellen und konfigurieren Sie eine Sicherheitsrolle wie folgt:

Erstellen Sie eine neue Sicherheitsrolle oder duplizieren Sie eine vorhandene.	Die Symantec Management-Plattform und einige Lösungen enthalten vordefinierte Sicherheitsrollen. Siehe "Vordefinierte Sicherheitsrollen" auf Seite 112. Wenn die vordefinierten Sicherheitsrollen nicht die Anforderungen Ihres Unternehmens erfüllen, können Sie neue Rollen erstellen oder die vorhandenen Rollen duplizieren, um so neue Rollen zu erstellen. Sie können dann die Privilegien und Berechtigungen wie gewünscht ändern. Siehe "So erstellen Sie eine neue Sicherheitsrolle oder duplizieren eine vorhandene" auf Seite 93.
Importieren Sie Domänengruppen und Benutzer über Active Directory.	Wenn Sie Domänengruppen aus Active Directory importieren, wird eine Sicherheitsrolle im Symantec Management Plattform-Server für die Domänengruppe erstellt, die Sie importieren möchten. Mitglieder dieser Domänengruppe, einschließlich Benutzer und Untergruppen, werden auch importiert. Benutzer werden als Konten erstellt, und Untergruppen werden als Rollen erstellt. Die Mitgliedschaftsbeziehung wird während des Importes beibehalten. Siehe "So importieren Sie Domänengruppen und Benutzer aus dem Active Directory" auf Seite 94.

Bei der Installation der Symantec Management-Plattform wird dem Administrator, der die Installation durchführt, automatisch die Symantec-Administratorrolle zugewiesen. Der Administrator kann dann neue Sicherheitsrollen erstellen, soweit erforderlich, und jeder Rolle die entsprechenden Privilegien und Berechtigungen zuweisen. Anschließend kann der Administrator jeden Benutzer einer oder mehreren Rollen zuweisen.

Symantec empfiehlt das Einrichten der Sicherheitsrollen, bevor Notification Server in Ihrem Produktionsnetzwerk bereitgestellt wird.

Diese Aufgabe ist ein Schritt beim Einrichten der Symantec Management-Plattform-Sicherheit.

Siehe "Einrichten der Sicherheit für die Symantec Management-Plattform" auf Seite 88.

So erstellen Sie eine neue Sicherheitsrolle oder duplizieren eine vorhandene

1. Klicken Sie in Symantec Management Console im Menü "Einstellungen" auf "Sicherheit > Kontoverwaltung".
2. Klicken Sie im linken Teilfenster unter "Kontoverwaltung" auf "Rollen".
3. Führen Sie auf der Seite "Rollen" im linken Teilfenster eine der folgenden Aktionen aus:

So erstellen Sie eine neue Rolle	Klicken Sie auf "Hinzufügen". Geben Sie in das Dialogfeld "Neue Rolle" den Namen der neuen Sicherheitsrolle ein und klicken Sie anschließend auf "OK". Die neue Rolle wird in der Liste der Rollen und die Standardeinstellungen werden im rechten Teilfenster angezeigt.
So duplizieren Sie eine vorhandene Rolle	Wählen Sie die Sicherheitsrolle aus, die Sie duplizieren möchten. Klicken Sie mit der rechten Maustaste auf die Rolle und klicken Sie auf "Duplizieren".

4 Konfigurieren Sie im rechten Teilfenster die entsprechenden Einstellungen auf den folgenden Registerkarten:

Mitglieder	Die der Rolle zugewiesenen Rollen und Benutzerkonten. Eine Rollenmitgliedschaft umfasst möglicherweise eine beliebige Anzahl von Benutzerkonten und Rollen. Die Mitglieder einer Rolle haben alle Privilegien bzw. Berechtigungen, die die Rolle gewährt. Siehe "Hinzufügen von Mitgliedern für eine Sicherheitsrolle" auf Seite 105.
Mitglied von	Die Sicherheitsrollen, zu denen die Rolle gehört. Die Rolle vereint die Berechtigungen und Privilegien dieser Rollen, kombiniert mit allen zusätzlichen Berechtigungen und Privilegien, die der Rolle direkt zugewiesen wurden. Siehe "Hinzufügen von Sicherheitsrollen als Mitglieder anderer Sicherheitsrollen" auf Seite 107.
Privilegien	Die Privilegien, die die Rolle seinen Mitgliedern gewährt. Mithilfe von Privilegien kann ein Benutzer eine bestimmte Aktion auf der Symantec Management-Plattform oder auf Elemente in der Symantec Management Console ausführen. In einigen Fällen muss das Benutzerkonto auch eine entsprechende Berechtigung für das Element haben. Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

5 (Optional) Wenn Sie den Sicherheitsrollenmanager zum Anzeigen oder Festlegen von Berechtigungen für die Sicherheitsrolle aufrufen möchten, klicken Sie auf Konsole 'Sicherheitsrollenmanager' anzeigen.

6 Klicken Sie auf "Änderungen speichern".

So importieren Sie Domänengruppen und Benutzer aus dem Active Directory

1 Klicken Sie in Symantec Management Console im Menü "Aktionen" auf "Erkennen > Microsoft Active Directory importieren".

2 Auf der Seite "Microsoft Active Directory-Import" in der Beschreibung, die mit "Rollen- und Kontoressourcen importieren aus <data source>, aus (kein)." gekennzeichnet ist. Um diesen Import im angegebenen Zeitplan durchzuführen, klicken auf die Benutzergruppe "(kein)".

3 (Optional) Erstellen Sie Ihre eigenen Regeln zum Importieren von Rolle und Konto.

4. Suchen Sie im Dialogfeld "Sicherheitsgruppen auswählen" nach den Domänengruppen, die Sie hinzufügen möchten, beispielsweise Administratoren und Benutzer.
5. Klicken Sie auf "Hinzufügen", um die ausgewählten Gruppen hinzuzufügen, und dann auf "OK".
6. Führen Sie die Regel als vollen Import aus, um die ausgewählte Domänengruppe zu importieren.
7. (Optional) Sie können einen vollen Import auch so planen, dass er in entsprechenden Abständen ausgeführt wird.

   Sie können diesen Zeitplan verwenden, um Ihre Sicherheitsrollenmitgliedschaft mit der Domänengruppenmitgliedschaft zu synchronisieren. Das heißt, wenn Sie einen Domänenbenutzer aus der Domänengruppe entfernen, wird das entsprechende Sicherheitskonto von der entsprechenden Sicherheitsrolle entfernt. Ebenso wird, wenn Sie einen Domänenbenutzer der Domänengruppe hinzufügen, das entsprechende Sicherheitskonto erstellt und zur entsprechenden Sicherheitsrolle hinzugefügt. Beachten Sie, dass, wenn ein Domänenbenutzer aus einer Domänengruppe entfernt wird, das entsprechende Sicherheitskonto nicht gelöscht wird. Nur die Mitgliedschaft bei der Sicherheitsrolle wird entfernt.
8. Klicken Sie in Symantec Management Console im Menü "Einstellungen" auf "Sicherheit > Kontoverwaltung".
9. Klicken Sie im linken Teilfenster im Ordner "Kontoverwaltung" auf "Rollen" und auf die Rolle, die Sie bearbeiten möchten.

10 (Optional) Konfigurieren Sie im rechten Teilfenster die entsprechenden Einstellungen auf den folgenden Registerkarten:

Mitglieder	Die der Rolle zugewiesenen Rollen und Benutzerkonten. Eine Rollenmitgliedschaft umfasst möglicherweise eine beliebige Anzahl von Benutzerkonten und Rollen. Die Mitglieder einer Rolle haben alle Privilegien bzw. Berechtigungen, die die Rolle gewährt. Siehe "Hinzufügen von Mitgliedern für eine Sicherheitsrolle" auf Seite 105. Beachten Sie, dass Sie Mitglieder der Rollen nicht manuell ändern dürfen, die Sie aus Active Directory importiert haben. Diese Beschränkung existiert, weil alle folgenden Regelausführungen die Mitgliedschaftskonfiguration überschreiben. Rollen, die Sie aus Active Directory importieren, sind so entworfen worden, dass sie dieselbe Mitgliedschaft wie die entsprechenden Domänengruppen beibehalten.
Mitglied von	Die Sicherheitsrollen, zu denen die Rolle gehört. Die Rolle vereint die Berechtigungen und Privilegien dieser Rollen, kombiniert mit allen zusätzlichen Berechtigungen und Privilegien, die der Rolle direkt zugewiesen wurden. Siehe "Hinzufügen von Sicherheitsrollen als Mitglieder anderer Sicherheitsrollen" auf Seite 107.
Privilegien	Die Privilegien, die die Rolle seinen Mitgliedern gewährt. Mithilfe von Berechtigungen kann ein Benutzer eine bestimmte Aktion auf der Symantec Management-Plattform oder für Elemente in der Symantec Management Console ausführen. In einigen Fällen muss das Benutzerkonto auch eine entsprechende Berechtigung für das Element haben. Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

11 (Optional) Wenn Sie den Sicherheitsrollenmanager zum Anzeigen oder Festlegen von Berechtigungen für die Sicherheitsrolle aufrufen möchten, klicken Sie auf Konsole 'Sicherheitsrollenmanager' anzeigen.

12 Klicken Sie auf "Änderungen speichern".

Zuweisen von Privilegien zu einer Sicherheitsrolle

Sie müssen die Privilegien angeben, die die einzelnen Sicherheitsrollen ihren Mitgliedern gewähren. Ein Recht ermöglicht einem Benutzer die Ausführung einer bestimmten Aktion auf der Symantec Management-Plattform oder an Elementen in der Symantec Management Console. Damit der Benutzer eine Aktion an einem Element ausführen kann, muss seine Rolle die notwendige Berechtigung für das Element haben. Wenn Sie zum Beispiel einer Rolle die Privilegien "Aufgabe starten" und "Aufgabe anhalten" zuweisen, müssen Sie ihr auch die Berechtigung zum Ausführen der entsprechenden Aufgaben zuweisen. Die Rolle kann nicht auf Aufgaben zugreifen, für die sie keine Ausführungsberechtigung erhalten hat.

Siehe "Zuweisen von Sicherheitsberechtigungen zu Ordnern und Elementen" auf Seite 108.

Rechte einer Sicherheitsrolle zuzuweisen ist ein Teil des Konfigurierens von Sicherheitsrollen. Diese Aufgabe ist ein Schritt bei dem Einrichten von Symantec Management-Plattform-Sicherheit.

Siehe "Erstellen und Konfigurieren von Sicherheitsrollen" auf Seite 91.

So weisen Sie einer Sicherheitsrolle Privilegien zu

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Sicherheit" > "Kontoverwaltung".
2. Klicken Sie im linken Teilfenster auf "Kontoverwaltung" > "Rollen".
3. Klicken Sie auf der Seite "Rollen" im linken Teilfenster auf die Sicherheitsrolle, die Sie konfigurieren möchten.
4. Wählen Sie im rechten Teilfenster auf der Registerkarte "Privilegien" die Privilegien, die Sie der Rolle zuweisen möchten.

   Um ein Recht auszuwählen, aktivieren Sie das entsprechende Kontrollkästchen.

   Siehe "Sicherheitsprivilegkategorien" auf Seite 510.
5. Klicken Sie auf "Änderungen speichern".

Erstellen und Konfigurieren von Benutzerkonten der Symantec Management-Plattform

Symantec Management-Plattform hat seine eigenen Benutzerkonten. In vorherigen Versionen von Symantec Management-Plattform 7.1 wurden Windows-Benutzer und -Gruppen für die Benutzersicherheit verwendet. Windows-Benutzer werden weiterhin verwendet, aber sie sind nicht mehr der einzige Sicherheitsmechanismus.

Benutzerkonten, auch als Benutzer bezeichnet, sind nicht dasselbe wie Benutzerressourcen in der Symantec Management-Plattform. Eine

Benutzerressource ist eine Entität, die verwendet wird, um verwaltete Geräte mit dem Besitzer des Geräts zu verknüpfen. Die vorhandenen Benutzerressourcen und die Benutzerkonten, die bei der Symantec Management Console einloggen oder einen Workflow ausführen können, sind separate Entitäten.

Ein Benutzerkonto für die Symantec Management-Plattform wird mit den Windows-Identifikationsdaten verknüpft, die der Benutzer benötigt, um auf die Symantec Management Console zuzugreifen. Außerdem kann das Benutzerkonto mit internen Identifikationsdaten verknüpft werden, die den Zugriff auf andere Dienste der Symantec Management-Plattform ermöglichen, zum Beispiel auf Workflows. Das Benutzerkonto kann zu den entsprechenden Sicherheitsrollen hinzugefügt werden: Ein Konto hat die Gesamtheit aller Privilegien und Berechtigungen, die durch die Rollen gewährt werden, zu denen es gehört.

Identifikationsdaten sind etwas, das ein Benutzerkonto zur Verfügung stellt, um seine Identität nachzuweisen. In der Symantec Management-Plattform sind mögliche Identifikationsdaten ein Benutzername und ein Kennwort oder ein Windows-Konto. Das Benutzerkonto verknüpft Identifikationsdaten mit einem bestimmten Benutzer und ermöglicht diesem den Zugriff auf die Symantec Management Console oder die Dienste der Symantec Management-Plattform.

Die Symantec Management-Plattform benutzt zwei Typen von Identifikationsdaten:

Interne Identifikationsdaten	Ermöglicht dem Benutzer den Zugriff auf die entsprechenden Dienste der Symantec Management-Plattform unter Verwendung eines Benutzernamens und eines Kennworts, die in der CMDB gespeichert werden. Aus Sicherheitsgründen wird nur der Hash-Wert des Kennworts gespeichert. Ein Benutzerkonto kann interne Identifikationsdaten nicht dazu verwenden, auf die Symantec Management Console zuzugreifen. Die internen Identifikationsdaten werden derzeit nur für die Workflow-Integration verwendet.

Windows-Identifikationsdaten	Ermöglicht dem Benutzer den Zugriff auf die Symantec Management Console und die Dienste der Symantec Management-Plattform unter Verwendung eines Windows-Benutzernamens und -Kennworts. Um Windows-Identifikationsdaten verwenden zu können, muss sich der Notification Server in der Domäne des Benutzers befinden oder die Domäne des Benutzers muss von der Notification Server-Domäne als vertrauenswürdig eingestuft werden. Sie sollten Windows-Identifikationsdaten konfigurieren, wenn Ihre Organisation intern Windows-Konten verwendet. Die Verwendung von Windows-Identifikationsdaten ermöglicht es Ihnen, Kennwortkomplexitätsforderungen durchzusetzen, Kennwörter regelmäßig zu ändern, einen Kennwortverlauf zu speichern und andere Kennwortverwaltungsaufgaben in Windows durchzuführen.

Sie können Ihre Symantec Management-Plattform-Benutzerkonten gemäß den Anforderungen Ihrer Organisation konfigurieren. Sie müssen alle gewünschten Konten erstellen und sie den entsprechenden Sicherheitsrollen zuweisen. Jedes Konto hat die Gesamtheit aller Privilegien und Berechtigungen, die durch die Rollen gewährt werden, zu denen es gehört.

Sie können ein Benutzerkonto mithilfe einer der folgenden Methoden erstellen und konfigurieren:

- Erstellen Sie ein neues Benutzerkonto oder duplizieren Sie ein vorhandenes Benutzerkonto.
- Importieren Sie Domänengruppen und Benutzer aus dem Active Directory.

Diese Aufgabe ist ein Schritt beim Einrichten der Symantec Management-Plattform-Sicherheit.

Siehe "Einrichten der Sicherheit für die Symantec Management-Plattform" auf Seite 88.

So erstellen Sie ein neues Benutzerkonto bzw. duplizieren ein vorhandenes Benutzerkonto

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Sicherheit" > "Kontoverwaltung".
2. Klicken Sie im linken Teilfenster auf "Kontoverwaltung" > "Konten".

3 Führen Sie auf der Seite "Konten" im linken Teilfenster eine der folgenden Aktionen aus:

So erstellen Sie ein neues Konto	Klicken Sie auf "Hinzufügen". Geben Sie im Dialogfeld "Neues Konto" den Namen des neuen Symantec Management-Plattform-Kontos ein und klicken Sie dann auf "OK". Das neue Konto erscheint in der Kontenliste. Standardmäßig ist der Status des neuen Kontos "Inaktiv".
So duplizieren Sie ein vorhandenes Konto	Klicken Sie mit der rechten Maustaste auf das Symantec Management-Plattform-Konto das Sie duplizieren und konfigurieren möchten. Geben Sie den Namen der neuen Kopie dieses Kontos ein und klicken Sie auf "OK".

4 Konfigurieren Sie im rechten Teilfenster die entsprechenden Einstellungen auf den folgenden Registerkarten:

Allgemein	Die allgemeinen Kontodetails. Dazu gehören der vollständige Name und die E-Mail-Adresse des Benutzers, für den das Konto erstellt wurde, der Kontostatus und die Kontoidentifikationsdaten. Siehe "Angeben allgemeiner Details für ein Symantec Management-Plattform-Benutzerkonto" auf Seite 101. Siehe "Konfigurieren von Identifikationsdaten für ein Symantec Management-Plattform-Benutzerkonto" auf Seite 102.
Mitglied von	Die Sicherheitsrollen, zu denen das Konto gehört. Das Konto hat die Gesamtheit aller Privilegien und Berechtigungen, die durch die Rollen gewährt werden, zu denen es gehört. Siehe "Zuweisen eines Symantec Management-Plattform-Benutzerkontos zu einer Sicherheitsrolle" auf Seite 106.

5 Klicken Sie auf "Änderungen speichern".

So importieren Sie Domänengruppen und Benutzer aus dem Active Directory

1. Klicken Sie in Symantec Management Console im Menü "Aktionen" auf "Erkennen > Microsoft Active Directory importieren".
2. Auf der Seite "Microsoft Active Directory-Import" in der Beschreibung, die mit "Rollen- und Kontoressourcen importieren aus <data source>, aus (kein)." gekennzeichnet ist. Um diesen Import im angegebenen Zeitplan durchzuführen, klicken auf die Benutzergruppe "(kein)".
3. (Optional) Erstellen Sie Ihre eigenen Regeln zum Importieren von Rolle und Konto.
4. Suchen Sie im Dialogfeld "Sicherheitsgruppen auswählen" die Domänengruppen, aus denen Sie Benutzerkonten importieren möchten; beispielsweise Administratoren und Benutzer.
5. Klicken Sie auf "Hinzufügen" und dann auf "OK", um die ausgewählten Gruppen hinzuzufügen.
6. Führen Sie die Regel als vollständigen Import aus, um die ausgewählten Domänengruppen zu importieren.
7. (Optional) Sie können einen vollständigen Import auch in regelmäßigen Abständen durchführen.

   Sie können diesen Zeitplan verwenden, um Ihre Sicherheitsrollenmitgliedschaft mit der Domänengruppenmitgliedschaft zu synchronisieren. Das heißt, wenn Sie einen Domänenbenutzer aus der Domänengruppe entfernen, wird das entsprechende Sicherheitskonto von der entsprechenden Sicherheitsrolle entfernt. Ebenso wird, wenn Sie einen Domänenbenutzer der Domänengruppe hinzufügen, das entsprechende Sicherheitskonto erstellt und zur entsprechenden Sicherheitsrolle hinzugefügt. Beachten Sie, dass, wenn ein Domänenbenutzer aus einer Domänengruppe entfernt wird, das entsprechende Sicherheitskonto nicht gelöscht wird. Nur die Mitgliedschaft bei der Sicherheitsrolle wird entfernt.

Video: Weitere Informationen zum Erstellen von Benutzerkonten der Symantec Management-Plattform finden Sie in dem Video Erstellen einer eingeschränkten ITMS-Administratorrolle auf Symantec Connect.

Angeben allgemeiner Details für ein Symantec Management-Plattform-Benutzerkonto

Sie müssen den vollständigen Namen und die E-Mail-Adresse des Benutzers angeben, für den das Konto erstellt wird. Außerdem können Sie bei Bedarf den Kontostatus von "Inaktiv" in "Aktiv" ändern.

Siehe "Erstellen und Konfigurieren von Benutzerkonten der Symantec Management-Plattform" auf Seite 233.

So geben Sie allgemeine Details für ein Symantec Management-Plattform-Benutzerkonto an

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Sicherheit" > "Kontoverwaltung".
2. Klicken Sie im linken Teilfenster auf "Kontoverwaltung" > "Konten".
3. Klicken Sie auf der Seite "Konten" im linken Teilfenster auf das Konto, das Sie konfigurieren möchten.
4. Geben Sie im rechten Teilfenster auf der Registerkarte "Allgemein" die Kontodetails an, indem Sie die entsprechenden Felder bearbeiten:

Vollständiger Name	Der vollständige Name des Benutzers, zu dem das Konto gehört.
E-Mail	Die E-Mail-Adresse des Kontobenutzers.

5. (Optional) Wenn Sie das Konto aktivieren oder deaktivieren möchten, klicken Sie auf das Statussymbol in der Titelleiste und wählen Sie dann "Aktiv" bzw. "Inaktiv".
6. Klicken Sie auf "Änderungen speichern".

Konfigurieren von Identifikationsdaten für ein Symantec Management-Plattform-Benutzerkonto

Sie müssen die entsprechenden Identifikationsdaten für jedes Symantec Management-Plattform-Benutzerkonto konfigurieren. Sie können einem Benutzerkonto einen Satz interne Identifikationsdaten für die Symantec Management-Plattform und einen Satz Windows-Identifikationsdaten hinzufügen. Die Windows-Identifikationsdaten emulieren das Verhalten von vorherigen Versionen der Symantec Management-Plattform.

Interne Identifikationsdaten ermöglichen dem Benutzer den Zugriff auf die entsprechenden Dienste der Symantec Management-Plattform unter Verwendung eines Benutzernamens und eines Kennworts, die in der CMDB gespeichert werden. Derzeit werden interne Identifikationsdaten nur für die Workflow-Integration verwendet.

Windows-Identifikationsdaten ermöglichen dem Benutzerkonto den Zugriff auf die Symantec Management Console und die Dienste der Symantec Management-Plattform unter Verwendung von Windows-Benutzername und

-Kennwort. Um Windows-Identifikationsdaten verwenden zu können, muss sich der Notification Server in der Domäne des Benutzers befinden oder die Domäne des Benutzers muss von der Notification Server-Domäne als vertrauenswürdig eingestuft werden.

Sie sollten Windows-Identifikationsdaten konfigurieren, wenn Ihre Organisation intern Windows-Konten verwendet. Die Verwendung von Windows-Identifikationsdaten ermöglicht es Ihnen, Kennwortkomplexitätsforderungen durchzusetzen, Kennwörter regelmäßig zu ändern, einen Kennwortverlauf zu speichern und andere Kennwortverwaltungsaufgaben in Windows durchzuführen.

Siehe "Erstellen und Konfigurieren von Benutzerkonten der Symantec Management-Plattform" auf Seite 233.

So konfigurieren Sie Identifikationsdaten für ein Symantec Management-Plattform-Benutzerkonto

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Sicherheit" > "Kontoverwaltung".
2. Klicken Sie im linken Teilfenster auf "Kontoverwaltung" > "Konten".
3. Klicken Sie auf der Seite "Konten" im linken Teilfenster auf das Konto, das Sie konfigurieren möchten.

4 Klicken Sie im rechten Teilfenster auf der Registerkarte "Allgemein" unter "Identifikationsdaten" auf "Identifikationsdaten hinzufügen" und führen Sie dann eine der folgenden Aktionen aus:

So fügen Sie dem Konto Windows-Identifikationsdaten hinzu	Klicken Sie auf "Windows" und geben Sie dann im Dialogfeld "Windows-Identifikationsdaten" den entsprechenden Windows-Benutzernamen im Format "Domäne/Benutzername" an. Wenn sich das Windows-Konto in derselben Domäne befindet wie der Notification Server, können Sie die Domäne auslassen und nur den Benutzernamen angeben. Wenn Sie ein Windows-Konto angeben, das bereits einem Benutzerkonto zugewiesen ist, werden die Windows-Identifikationsdaten aus dem vorhandenen Konto entfernt. Anschließend werden die Windows-Identifikationsdaten dem neuen Benutzerkonto hinzugefügt.
So fügen Sie dem Konto interne Identifikationsdaten hinzu	Klicken Sie auf "Intern" und geben Sie dann im Dialogfeld "Interne Identifikationsdaten erstellen" das entsprechende Kennwort an. Das Kennwort muss die Kennwortkomplexitätseinstellungen erfüllen. Siehe "Konfigurieren von Kennwortkomplexitäts- und Sperreinstellungen" auf Seite 115. Der in den Identifikationsdaten angegebene Benutzername ist der Name des Symantec Management-Plattform-Kontos und kann nicht geändert werden.

5 Klicken Sie auf "OK".

Die neuen Identifikationsdaten werden zur Liste "Identifikationsdaten" hinzugefügt.

6 (Optional) Wenn Sie Identifikationsdaten ändern möchten, wählen Sie sie in der Liste "Identifikationsdaten" aus und klicken Sie dann auf "Bearbeiten". Nehmen Sie im Dialogfeld "Windows-Identifikationsdaten bearbeiten" oder im Dialogfeld "Interne Identifikationsdaten bearbeiten" die entsprechenden Änderungen vor und klicken Sie anschließend auf "OK".

   Aus Sicherheitsgründen wird im Dialogfeld "Interne Identifikationsdaten bearbeiten" nicht das aktuelle Kennwort angezeigt. Wenn Sie ein neues Kennwort angeben, werden die Identifikationsdaten entsprechend aktualisiert. Wenn Sie das Feld "Kennwort" leer lassen, wird das ursprüngliche Kennwort beibehalten.

7 (Optional) Wenn Sie Identifikationsdaten löschen möchten, wählen Sie sie in der Liste "Identifikationsdaten" aus und klicken Sie dann auf "Löschen".

8 Klicken Sie auf "Änderungen speichern".

Hinzufügen von Mitgliedern für eine Sicherheitsrolle

Sie müssen die entsprechenden Mitglieder (Benutzerkonten und andere Sicherheitsrollen) jeder Sicherheitsrolle zuweisen . Um Mitglieder hinzufügen zu können, müssen Sie Mitglied der Symantec-Administratorrolle sein oder Mitglied einer Rolle, die das Recht "Sicherheit ändern" hat. Sie können ein Benutzerkonto einer beliebigen Anzahl von Sicherheitsrollen zuweisen. Die Mitglieder einer Rolle haben alle Privilegien und Berechtigungen, die der Rolle gewährt werden.

Sie können eine Rolle mehreren Sicherheitsrollen hinzufügen, aber Sie können keine zirkuläre Mitgliedschaft nicht erstellen, bei der eine Rolle Mitglied von sich selbst wird. Ein Mitglied mehrerer Sicherheitsrollen verfügt über die Kombination aller Privilegien und Berechtigungen, die diese Rollen gewähren.

Mitglieder einer Sicherheitsrolle hinzuzufügen ist ein Teil des Konfigurierens von Sicherheitsrollen. Diese Aufgabe ist ein Schritt beim Einrichten der Sicherheit für die Symantec Management-Plattform.

Siehe "Erstellen und Konfigurieren von Sicherheitsrollen" auf Seite 91.

So fügen Sie einer Sicherheitsrolle Mitglieder hinzu

1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Sicherheit" > "Kontoverwaltung".

2 Klicken Sie im linken Teilfenster auf "Kontoverwaltung" > "Rollen".

3 Klicken Sie auf der Seite "Rollen" im linken Teilfenster auf die Sicherheitsrolle, die Sie konfigurieren möchten.

4 Klicken Sie im rechten Teilfenster auf der Registerkarte "Mitglieder" auf "Mitglied hinzufügen" und führen Sie dann eine der folgenden Aktionen aus:

So fügen Sie der Rolle ein Benutzerkonto hinzu	Klicken Sie auf "Konto hinzufügen".
So fügen Sie der Rolle eine weitere Sicherheitsrolle hinzu	Klicken Sie auf "Rolle hinzufügen".

5 Wählen Sie im Dialogfeld "Konto/Konten auswählen" oder "Rolle(n) auswählen" die Benutzerkonten bzw. Sicherheitsrollen, die Sie hinzufügen möchten, und klicken Sie dann auf "OK".

6 Überprüfen Sie auf der Registerkarte "Mitglieder", ob die Mitgliederliste korrekt ist. Sie können Mitglieder nach Bedarf entfernen.

7 Klicken Sie auf "Änderungen speichern".

Zuweisen eines Symantec Management-Plattform-Benutzerkontos zu einer Sicherheitsrolle

Sie müssen jedes Symantec Management-Plattform-Benutzerkonto den entsprechenden Sicherheitsrollen zuweisen. Um eine Rollenmitgliedschaft zuweisen zu können, müssen Sie Mitglied der Symantec-Administratorrolle sein oder Mitglied einer Rolle, die das Recht "Sicherheit ändern" hat. Das Konto hat die Gesamtheit aller Privilegien und Berechtigungen, die durch die Rollen gewährt werden, zu denen es gehört.

Siehe "Erstellen und Konfigurieren von Benutzerkonten der Symantec Management-Plattform" auf Seite 233.

So weisen Sie ein Symantec Management-Plattform-Konto einer Sicherheitsrolle zu

1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Sicherheit" > "Kontoverwaltung".

2 Klicken Sie im linken Teilfenster auf "Kontoverwaltung" > "Konten".

3 Klicken Sie auf der Seite "Konten" im linken Teilfenster auf das Konto, das Sie konfigurieren möchten.

4 Wählen Sie im rechten Teilfenster auf der Registerkarte "Mitglied von" die entsprechenden Einstellungen.

5 Klicken Sie auf "Rolle hinzufügen".

6 Wählen Sie im Dialogfeld "Rolle(n) auswählen" die Sicherheitsrollen, denen Sie das Konto hinzufügen möchten, und klicken Sie dann auf "OK".

7 Überprüfen Sie auf der Registerkarte "Mitglied von", ob die Liste der Sicherheitsrollen korrekt ist. Sie können Sicherheitsrollen nach Bedarf entfernen.

8 Klicken Sie auf "Änderungen speichern".

Hinzufügen von Sicherheitsrollen als Mitglieder anderer Sicherheitsrollen

Sie können eine Rolle als Mitglied anderer Sicherheitsrollen hinzufügen. Um eine Rollenmitgliedschaft zuweisen zu können, müssen Sie Mitglied der Symantec-Administratorrolle sein oder Mitglied einer Rolle, die das Recht "Sicherheit ändern" hat. Sie können eine Rolle mehreren Sicherheitsrollen hinzufügen, aber Sie können keine zirkuläre Mitgliedschaft nicht erstellen, bei der eine Rolle Mitglied von sich selbst wird. Einer Rolle wird die Gesamtheit aller Privilegien und Berechtigungen gewährt, die die Rollen bereitstellen, zu denen sie gehört.

Eine Rolle als Mitglied einer anderen Rolle hinzuzufügen ist dasselbe wie die Rolle zur Mitgliedschaft der anderen Rolle hinzuzufügen. Mithilfe diese Methode können Sie eine bestimmte Rolle in einem einzigen Verfahren mehreren Rollen hinzufügen. Die Alternative wäre, alle anderen Rollen zu konfigurieren und die Rolle speziell der Mitgliedschaft jeder einzelnen hinzuzufügen.

Sicherheitsrollen als Mitglieder anderer Sicherheitsrollen hinzuzufügen ist ein Teil des Konfigurierens von Sicherheitsrollen. Diese Aufgabe ist ein Schritt beim Einrichten der Symantec Management-Plattform-Sicherheit.

Siehe "Erstellen und Konfigurieren von Sicherheitsrollen" auf Seite 91.

So fügen Sie eine Sicherheitsrolle als Mitglied anderer Sicherheitsrollen hinzu

1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Sicherheit" > "Kontoverwaltung".

2 Klicken Sie im linken Teilfenster auf "Kontoverwaltung" > "Rollen".

3 Klicken Sie auf der Seite "Rollen" im linken Teilfenster auf die Sicherheitsrolle, die Sie konfigurieren möchten.

4 Konfigurieren Sie im rechten Teilfenster auf der Registerkarte "Mitglied von" die entsprechenden Einstellungen.

5 Klicken Sie auf "Rolle hinzufügen".

6 Wählen Sie im Dialogfeld "Rolle(n) auswählen" die Sicherheitsrollen, denen Sie die Rolle hinzufügen möchten, und klicken Sie dann auf "OK".

7 Überprüfen Sie auf der Registerkarte "Mitglied von", ob die Liste der Sicherheitsrollen korrekt ist. Sie können Sicherheitsrollen nach Bedarf entfernen.

8 Klicken Sie auf "Änderungen speichern".

Zuweisen von Sicherheitsberechtigungen zu Ordnern und Elementen

Sie können die nicht geerbten Berechtigungen für jeden Ordner und jedes Element für die einzelnen Sicherheitsrollen angeben. Diese werden mit den vom übergeordneten Ordner geerbten Berechtigungen kombiniert. Die kombinierten Berechtigungen legen den Zugriff fest, den die Sicherheitsrolle für den betreffenden Ordner bzw. das Element hat. Standardmäßig erben alle untergeordneten Ordner und Elemente die kombinierten Berechtigungssätze.

Siehe "Zugriff auf den Sicherheitsrollenmanager" auf Seite 119.

Diese Aufgabe ist ein Schritt beim Einrichten der Sicherheit für die Symantec Management-Plattform.

Siehe "Einrichten der Sicherheit für die Symantec Management-Plattform" auf Seite 88.

So weisen Sie Sicherheitsberechtigungen für Ordner und Elemente zu

1. Wählen Sie im Sicherheitsrollenmanager in der Dropdown-Liste "Rollen" die Sicherheitsrolle aus, für die Sie Berechtigungen festlegen möchten.
2. (Optional) Wählen Sie in der Dropdown-Liste "Ansicht" eine Elementkategorie zum Anzeigen der Ordnerstruktur aus, die die relevanten Elemente enthält.

   Wenn Sie die vollständige Ordnerstruktur anzeigen möchten, wählen Sie "Alle Elemente".
3. Wählen Sie im linken Bereich den Ordner bzw. das Element aus, für den/das Sie Berechtigungen festlegen möchten.

   Beachten Sie, dass einige Elemente standardmäßig ausgeblendet sein könnten. Klicken Sie zum Anzeigen aller Elemente in der Symbolleiste auf das Symbol "Verborgene Elemente anzeigen". Diese Funktion ist nur für Rollen verfügbar, denen das Privileg "Sicherheit ändern" zugewiesen ist.

   Warnung: Gehen Sie beim Bearbeiten der Sicherheitsberechtigungen eines verborgenen Elements sorgfältig vor, da sie nicht darauf ausgelegt sind, geändert zu werden.

   ---
4. Nehmen Sie im rechten Teilfenster im Bereich "Nicht geerbt" die entsprechenden Änderungen an den Berechtigungseinstellungen vor.
5. (Optional) Wenn Sie die Berechtigungsvererbung für einen Ordner oder ein Element konfigurieren möchten, klicken Sie auf "Erweitert".

   Siehe "Anpassen der Vererbungsregeln für Berechtigungen" auf Seite 109.
6. Klicken Sie auf "Änderungen speichern".

Anpassen der Vererbungsregeln für Berechtigungen

Standardmäßig ist die Berechtigungsvererbung für alle Ordner und Elemente aktiviert. Untergeordnete Ordner und Elemente erben die Sicherheitsberechtigungen für jede Rolle, die einem Ordner zugewiesen wird. Die geerbten Berechtigungen der untergeordneten Ordner und Elemente können nicht geändert werden, es können jedoch zusätzliche, nicht geerbte Berechtigungen zugewiesen werden. Die nicht geerbten Berechtigungen werden direkt auf den Ordner bzw. das Element angewendet und können jederzeit geändert werden. Die Berechtigungseinstellungen für jeden Ordner bzw. jedes Element sind eine Kombination aus geerbten und nicht geerbten Einstellungen. Die kombinierten Berechtigungssätze werden dann auf alle untergeordneten Ordner und Elemente angewendet. Jegliche Änderungen der Berechtigungseinstellungen für einen Ordner werden sofort auf dessen untergeordnete Ordner und Elemente angewendet.

Sie können die Berechtigungsvererbung für beliebige Ordner und Elemente deaktivieren. Damit können Sie einige der geerbten Berechtigungen von dem Ordner bzw. Element entfernen, aber für den übergeordneten Ordner beibehalten. Die auf einen Ordner oder ein Element anwendeten Berechtigungsvererbungseinstellungen gelten für jede Sicherheitsrolle. Sie können Vererbungseinstellungen nicht für bestimmte Rollen anpassen.

Warnung: Die Deaktivierung der Berechtigungsvererbung für einen Ordner oder ein Element kann zur unerwarteten Zugriffsverweigerung für Benutzerkonten führen. Wenn Sie Berechtigungsvererbung deaktivieren, stellen Sie sicher, dass es ausdrücklich angegebene Berechtigungen für den Ordner bzw. das Element gibt, damit Benutzerkonten den entsprechenden Zugriff haben.

Außerdem können Sie alle nicht geerbten Berechtigungen für Ordner und Elemente deaktivieren, sodass nur die geerbten Berechtigungen übrig bleiben. Sie sollten alle nicht geerbten Berechtigungen entfernen, um benutzerdefinierte Berechtigungen zu entfernen, die den untergeordneten Ordnern oder Elementen hinzugefügt wurden. Sie können diese Funktion auch verwendet, um einen Standardsatz von Berechtigungen für alle untergeordneten Ordner oder Elemente wiederherzustellen.

Siehe "Zuweisen von Sicherheitsberechtigungen zu Ordnern und Elementen" auf Seite 108.

Diese Aufgabe ist ein Schritt beim Einrichten der Sicherheit für die Symantec Management-Plattform.

Siehe "Einrichten der Sicherheit für die Symantec Management-Plattform" auf Seite 88.

So passen Sie die Berechtigungs-Vererbungsregeln für Ordner oder Elemente an

1. Wählen Sie im linken Bereich des Sicherheitsrollenmanagers den Ordner bzw. das Element aus, für den/das Sie die Berechtigungsvererbung konfigurieren möchten.
2. Klicken Sie im rechten Teilfenster auf "Erweitert".
3. Klicken Sie im Fenster "Berechtigungen für:" Wählen Sie im Fenster *"Elementname"* in der Liste "Konto/Gruppe/Rolle" die Sicherheitsrolle oder das Benutzerkonto aus, für die bzw. das Sie Berechtigungen konfigurieren möchten.

   Wenn Sie der Liste eine andere Sicherheitsrolle oder ein anderes Benutzerkonto hinzufügen möchten, klicken Sie auf "Hinzufügen". Wählen Sie im Dialogfeld "Trustees hinzufügen" die entsprechende Sicherheitsrolle bzw. das entsprechende Benutzerkonto aus.
4. (Optional) Ändern Sie im Bereich "Berechtigungen für:" die Berechtigungen, die der ausgewählten Sicherheitsrolle für diesen Ordner bzw. dieses Element zugewiesen sind.

   Sie können diese Funktion nur für nicht geerbte Berechtigungen verwenden. Geerbte Berechtigungen können nicht bearbeitet werden.

5 Führen Sie eine der folgenden Aktionen aus:

So werden Berechtigungen vom übergeordneten Ordner vererbt	Aktivieren Sie die Option Für untergeordnete Objekte geltende Berechtigungseinträge vom übergeordneten Objekt erben". Die geerbten Berechtigungseinstellungen für den Ordner bzw. das Element werden auf die jeweiligen Berechtigungseinstellungen des übergeordneten Ordners aktualisiert.
So wird die Berechtigungsvererbung deaktiviert	Deaktivieren Sie die Option Für untergeordnete Objekte geltende Berechtigungseinträge vom übergeordneten Objekt erben". Sie können entweder die aktuellen geerbten Berechtigungen vom übergeordneten Ordner kopieren oder alle geerbten Berechtigungen entfernen. Nachfolgende Änderungen an den Berechtigungseinstellungen für den übergeordneten Ordner haben keine Auswirkungen auf die Berechtigungseinstellungen für den Ordner bzw. das Element.
So entfernen Sie alle nicht geerbten Berechtigungen von untergeordneten Ordnern und Elementen	Aktivieren Sie die Option "Berechtigungen für alle untergeordneten Objekte ersetzen". Die nicht geerbten Berechtigungseinstellungen werden für alle untergeordneten Ordner und Elemente gelöscht, und es bleiben nur die geerbten Berechtigungen übrig.

6 Klicken Sie auf "Änderungen speichern".

7 (Optional) Wenn Sie die Vererbung von Berechtigungen im Dialogfeld "Verhalten für geerbte Berechtigungen" deaktiviert haben, klicken Sie auf die entsprechende Option:

"Kopieren"	Die aktuellen geerbten Berechtigungen werden mit den nicht geerbten Berechtigungseinstellungen für diesen Ordner bzw. dieses Element zusammengeführt.
Entfernen	Die aktuellen geerbten Berechtigungen werden gelöscht, und es bleiben nur die nicht geerbten Berechtigungen übrig. Vergewissern Sie sich, dass Sie die richtigen nicht geerbten Berechtigungen für den Ordner bzw. das Element haben, bevor Sie diese Option wählen.

8 Klicken Sie auf "Abbrechen", um das Fenster "Berechtigungen für:" *Elementname* zu schließen.

Vordefinierte Sicherheitsrollen

Die Symantec Management-Plattform enthält einen Satz vordefinierter Sicherheitsrollen, die Sie verwenden können. Wenn diese vordefinierten Sicherheitsrollen den Anforderungen Ihres Unternehmens nicht genügen, können Sie neue erstellen. Außerdem können Sie die vordefinierten Sicherheitsrollen durch Angeben anderer Privilegien und Berechtigungen anpassen.

Siehe "Erstellen und Konfigurieren von Sicherheitsrollen" auf Seite 91.

Tabelle 4-2 Vordefinierte Sicherheitsrollen für Symantec Management-Plattform

Sicherheitsrolle	Beschreibung
Alle	Eine Rolle der obersten Ebene, die alle Rollen und Benutzerkonten enthält. Die Mitgliedschaft dieser Rolle wird automatisch berechnet und kann nicht manuell geändert werden. Standardmäßig sind dieser Rolle keine Privilegien zugewiesen. Wenn Sie Berechtigungen und Privilegien für diese Rolle ändern, werden die Änderungen automatisch auf allen anderen Rollen und Benutzerkonten angewendet.
Symantec-Administratoren	Umfasst alle Sicherheitsprivilegien und Berechtigungen, hat also vollständigen Zugriff auf alle Aspekte der Symantec Management-Plattform und aller installierten Lösungen. Sie können die Mitgliedschaft dieser Sicherheitsrolle ändern, aber nicht ihre Privilegien und Berechtigungen.

Sicherheitsrolle	Beschreibung
Symantec-Vorgesetzte	Hat alle Verwaltungs- und die meisten Kontextmenürechte. Hat begrenzte Systemrechte. Hat die Leseberechtigung auf Ressourcen, einschließlich Sicherheitsressourcen. Hat vollen Zugriff auf Cloud-fähige Verwaltungseinstellungen, einschließlich Einrichten eines neuen Internet-Gateway und Erzeugen des Installationspakets für den Symantec Management-Agent.
Benutzer der Symantec-Stufe 2	Hat die vollständigen Verwaltungsprivilegien und die meisten Kontextmenüprivilegien zugewiesen. Hat Leserecht auf Ressourcen, ausschließlich Sicherheitsressourcen. Hat eingeschränkten Zugriff auf Cloud-fähige Verwaltungseinstellungen. Beispiel: "Symantec-Mitarbeiter Stufe 2" können die Richtlinie "Einstellungen für die Cloud-fähige Verwaltung".
Benutzer der Symantec-Stufe 1	Hat keine Privilegien zugewiesen. Hat Leserecht auf Ressourcen, ausschließlich Sicherheitsressourcen.
Symantec-Softwarebibliothekar	Hat die Software Management Framework-Privilegien und die Kontextmenü-Aktionsprivilegien zugewiesen. Die Privilegien sind begrenzt auf die zur Erstellung und Verwaltung von Softwarepaketen erforderlichen Privilegien.
Symantec-Gäste	Hat keine Privilegien zugewiesen. Hat Leserecht für Berichte.
NT-Autorität\Authentifizierte Benutzer	Benutzer, die sich bei der Symantec Management Console einloggen, werden automatisch Mitglied dieser Rolle. Die Mitgliedschaft dieser Rolle wird automatisch berechnet und kann nicht manuell geändert werden. Standardmäßig sind dieser Rolle keine Privilegien oder Berechtigungen zugewiesen.

Sicherheitsverwaltungsaufgaben für Symantec Management-Plattform

Tabelle 4-3 Sicherheitsverwaltungsaufgaben für Symantec Management-Plattform

Aufgabe	Beschreibung
Konfigurieren Sie Kennwortkomplexitäts- und Sperreinstellungen.	Sie müssen entsprechende Kennwortkomplexitätsanforderungen festlegen, um zu verhindern, dass für Benutzerkonten der Symantec Management-Plattform schwache Kennwörter erstellt werden. Änderungen, die Sie an den Kennwortkomplexitätseinstellungen vornehmen, gelten nicht für vorhandene Kennwörter. Die Kennwortkomplexitätsregeln werden nur dann angewendet, wenn Kennwörter erstellt oder geändert werden. Siehe "Konfigurieren von Kennwortkomplexitäts- und Sperreinstellungen" auf Seite 115.
Entsperren Sie gesperrte Identifikationsdaten.	Sie können die internen Identifikationsdaten freigeben, die gesperrt wurden, nachdem die Höchstzahl von erfolglosen Login-Versuchen überschritten wurde. Siehe "Freigeben von gesperrten Identifikationsdaten" auf Seite 118.
Anzeigen und Verwalten von Berechtigungen für Sicherheitsrollen.	Im Sicherheitsrollenmanager können Sie Berechtigungen für Sicherheitsrollen anzeigen und festlegen. Außerdem können Sie mit dem Sicherheitsrollenmanager ein Element in Besitz nehmen. Siehe "Zugriff auf den Sicherheitsrollenmanager" auf Seite 119.
Nehmen Sie einen Ordner oder ein Element in Besitz.	Sie können ein Element in Besitz nehmen, wenn seine Berechtigungen versehentlich entfernt wurden und der Besitzer nicht mehr darauf zugreifen kann. Nachdem Sie sie in Besitz genommen haben, können Sie die entsprechenden Berechtigungen zurücksetzen und den Zugriff für den ursprünglichen Besitzer wiederherstellen. Siehe "Besitznahme über Ordner oder Elemente" auf Seite 120.

Aufgabe	Beschreibung
Verwalten Sie Identifikationsdaten.	Verwaltungslösungen erstellen normalerweise Identifikationsdaten, wenn sie zur Durchführung einer Aufgabe erforderlich sind. Siehe "Verwalten von Identifikationsdaten" auf Seite 121.

Konfigurieren von Kennwortkomplexitäts- und Sperreinstellungen

Auf der Seite "Kennworteinstellungen" können Sie die Kennwortkomplexitäts- und Sperreinstellungen für interne Identifikationsdaten konfigurieren. Diese Einstellungen gelten nur für interne Identifikationsdaten: Sie gelten nicht für Kennwörter, die extern verwaltet werden, zum Beispiel ein Windows-Konto. Diese Komplexitäts- und Sperreinstellungen sind häufig erforderlich, um die Zugriffskontrollrichtlinie einer Organisation einzuhalten.

Sie müssen entsprechende Kennwortkomplexitätsanforderungen angeben, um zu verhindern, dass für Benutzerkonten der Symantec Management-Plattform schwache Kennwörter erstellt werden.

Hinweis: Änderungen, die Sie an den Kennwortkomplexitätseinstellungen vornehmen, gelten nicht für vorhandene Kennwörter. Die Kennwortkomplexitätsregeln werden nur dann angewendet, wenn Kennwörter erstellt oder geändert werden.

Sie können keine zeitlichen Einschränkungen angeben, zum Beispiel dass sich Benutzerkonten nur während bestimmter Zeiträume oder an bestimmten Tagen der Woche einloggen dürfen. Um diese Art von Einschränkung zu konfigurieren, können Sie eine geplante Aufgabe, einen Workflow oder eine Automatisierungsrichtlinie verwenden, durch die Konten zu den entsprechenden Zeiten deaktiviert und aktiviert werden.

Sie können kein maximales Kennwortalter für interne Identifikationsdaten konfigurieren. Das maximale Kennwortalter für Windows-Identifikationsdaten sollte mithilfe einer Windows-Richtlinie verwaltet werden.

Siehe "Freigeben von gesperrten Identifikationsdaten" auf Seite 118.

Sie müssen entsprechende Kennwortsperrbedingungen angeben, um einen nicht autorisierten Zugriff auf die Symantec Management-Plattform zu verhindern. Änderungen, die Sie an den Kennwortsperreinstellungen vornehmen, werden auf alle nachfolgenden fehlgeschlagenen Login-Versuche angewendet. Die Einstellung für die maximal zulässigen erfolglosen Versuche wird nicht auf die Anzahl der vorangegangenen fehlgeschlagenen Login-Versuche angewendet.

So konfigurieren Sie Kennwortkomplexitäts- und Sperreinstellungen

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Sicherheit" > "Kontoverwaltung".
2. Klicken Sie im linken Teilfenster auf "Kontoverwaltung" > "Kennworteinstellungen".
3. Konfigurieren Sie auf der Seite "Kennworteinstellungen" auf der Registerkarte "Kennwortkomplexität" die Kennwortkomplexitätseinstellungen:

Leeres Kennwort zulassen	Damit können Sie angeben, ob Identifikationsdaten ein leeres Kennwort haben können. Wenn Sie diese Einstellung aktivieren, ist die minimale Kennwortlänge deaktiviert. Standardmäßig ist diese Einstellung deaktiviert.
Mindestlänge des Kennworts	Damit können Sie die Mindestzahl von Zeichen angeben, die das Kennwort enthalten muss. Wenn Sie die Länge auf null (0) setzen möchten, müssen Sie außerdem die Einstellung "Leeres Kennwort zulassen" aktivieren. Der Standardwert ist sechs (6).
Mindestanzahl nicht alphabetischer Zeichen	Damit können Sie die Mindestzahl nicht alphabetischer Zeichen angeben, die das Kennwort enthalten muss. Nichtalphabetische Zeichen sind Zahlen (zum Beispiel 1, 2, 3 etc.) und Sonderzeichen (zum Beispiel !, ?, & etc.). Der Standardwert ist eins (1).
Kontoname muss enthalten sein	Damit können Sie angeben, ob das Kennwort den Benutzerkontonamen enthalten kann. Beachten Sie, dass hierbei die Groß- und Kleinschreibung ignoriert wird. Standardmäßig ist diese Einstellung deaktiviert.

4 Geben Sie auf der Seite "Kennworteinstellungen" auf der Registerkarte "Kennwortsperre" die entsprechenden Bedingungen für die Kennwortsperre an:

Identifikationsdatensperre aktivieren	Gibt an, ob die Identifikationsdaten gesperrt werden sollen, wenn die angegebene Höchstzahl von erfolglosen Login-Versuchen erreicht ist. Standardmäßig ist diese Einstellung aktiviert.
Sperrgrenzwert interne Identifikationsdaten	Gibt die Höchstzahl von Login-Versuchen an, die ein Benutzer mit bestimmten Identifikationsdaten erreichen darf. Wenn ein Benutzer häufiger als durch diesen Wert angegeben versucht, sich mit einem falschen Kennwort zu authentifizieren, werden die Identifikationsdaten für die angegebene Sperrzeit gesperrt. Erfolglose Login-Versuche werden ab dem Zeitpunkt gezählt, zu dem die Identifikationsdaten erstellt werden. Die erfolglosen Versuche müssen nicht innerhalb eines minimalen Zeitraums auftreten. Es gibt keine maximale Zeit, nach der ein erfolgloser Versuch nicht mehr gezählt wird. Wenn Sie diese Einstellung ändern, um die Höchstzahl der zulässigen erfolglosen Versuchen zu reduzieren, wird der neue Wert erst beim nächsten Login-Versuch auf ein Konto angewendet. Wenn der nächste Versuch erfolgreich ist, wird der Zähler auf null zurückgesetzt. (Alle vorherigen erfolglosen Versuche werden gelöscht.) Wenn jedoch der nächste Versuch fehlschlägt, wird der Zähler für die erfolglosen Versuche ausgewertet. Wenn die Höchstzahl erreicht (oder möglicherweise bereits überschritten) ist, wird das Konto gesperrt.

Sperrdauer	Gibt die Dauer an, für die gesperrte Identifikationsdaten nicht verwendet werden können. Der Standardzeitraum ist 1800 Minuten (30 Stunden). Alle Login-Versuche, die der Benutzer während dieses Zeitraums ausführt, schlagen fehl, selbst wenn die richtigen Identifikationsdaten angegeben werden. Wenn die Sperrzeit abläuft, sind die gleichen Identifikationsdaten wieder gültig. Es ist keine automatische Kennwortzurücksetzung erforderlich. Sie können eine unbegrenzte Sperrzeit angeben, indem Sie den Wert "-1" eingeben. In diesem Szenario bleiben gesperrte Identifikationsdaten gesperrt, bis ein Administrator sie manuell freigibt. Siehe "Freigeben von gesperrten Identifikationsdaten" auf Seite 118.

5 Klicken Sie auf "Änderungen speichern".

Siehe "Sicherheitsverwaltungsaufgaben für Symantec Management-Plattform" auf Seite 114.

Freigeben von gesperrten Identifikationsdaten

Auf der Seite "Identifikationsdaten freigeben" können Sie interne Identifikationsdaten freigeben, die gesperrt wurden, nachdem die Höchstzahl von erfolglosen Login-Versuchen überschritten wurde.

Siehe "Konfigurieren von Kennwortkomplexitäts- und Sperreinstellungen" auf Seite 115.

So geben Sie gesperrte Identifikationsdaten frei

1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Sicherheit" > "Kontoverwaltung".

2 Klicken Sie im linken Teilfenster auf "Kontoverwaltung" > "Identifikationsdaten freigeben".

3 Wählen Sie auf der Seite "Identifikationsdaten freigeben" in der Liste der gesperrten Identifikationsdaten diejenigen, die Sie freigeben möchten.

4 Klicken Sie auf "Identifikationsdaten freigeben".

Zugriff auf den Sicherheitsrollenmanager

Der Sicherheitsrollenmanager ist eine spezielle Konsole, mit der Sie Sicherheitsrollen anzeigen und Berechtigungen dafür einstellen können. In der Konsole können Sie eine bestimmte Sicherheitsrolle auswählen und die für jedes Element für diese Sicherheitsrolle zugeordneten Berechtigungen anzeigen. Sie können die Elemente nach Typ anzeigen oder alle verfügbaren Elemente und den Ordner bzw. das Element auswählen, für den/das Berechtigungen eingestellt werden sollen. Standardmäßig erben untergeordnete Elemente und Ordner alle Berechtigungen für einen Ordner. Sie können die Berechtigungsvererbung Ihren Anforderungen entsprechend ändern.

Außerdem können Sie mit Hilfe des Sicherheitsrollenmanagers von einem Element Besitz ergreifen. Sie müssen möglicherweise Besitz ergreifen, wenn Berechtigungen für ein Element versehentlich entfernt wurden und der Besitzer keinen Zugriff mehr darauf hat. Durch die Besitzergreifung eines Elements können Sie die geeigneten Berechtigungen zurücksetzen und den Zugriff für den ursprünglichen Besitzer wiederherstellen.

Tabelle 4-4 Methoden zum Zugriff auf den Sicherheitsrollenmanager

Option	Beschreibung
Direkt im Menü Einstellungen der Symantec Management Console	Wenn der Sicherheitsrollenmanager geöffnet wird, ist Ihre Sicherheitsrolle bereits ausgewählt und die Ansicht Alle Datenklassen wird angezeigt.
Im rechten Teilfenster der Seite Rollen	Wenn der Sicherheitsrollenmanager geöffnet wird, ist die geeignete Sicherheitsrolle bereits ausgewählt und die Ansicht Alle Datenklassen wird angezeigt.
Im Menü Aktionen für eine Sicherheitsrolle	Wenn der Sicherheitsrollenmanager geöffnet wird, ist die geeignete Sicherheitsrolle bereits ausgewählt und die Ansicht Alle Datenklassen wird angezeigt.
Im Kontextmenü für ein Element oder einen Ordner im linken Teilfenster	Normalerweise würden Sie diese Methode zum Festlegen von Berechtigungen für ein bestimmtes Element oder einen bestimmten Ordner verwenden. Wenn der Sicherheitsrollenmanager geöffnet wird, sind Ihre Sicherheitsrolle sowie der entsprechende Ordner bereits ausgewählt.

So greifen Sie vom Symantec Management Console-Menü aus auf den Sicherheitsrollenmanager zu

- Klicken Sie in der Symantec Management Console im Menü Einstellungen auf Sicherheit > Berechtigungen.

So greifen Sie von einer bestimmten Sicherheitsrolle aus auf den Sicherheitsrollenmanager zu

1. Klicken Sie in der Symantec Management Console im Menü Einstellungen auf Sicherheit > Kontoverwaltung.
2. Klicken Sie im linken Teilfenster auf "Kontoverwaltung" > "Rollen".
3. Klicken Sie auf der Seite Rollen im linken Teilfenster auf die Sicherheitsrolle, die Sie konfigurieren möchten.
4. Führen Sie einen der folgenden Schritte durch:
   - Im rechten Teilfenster klicken Sie auf "Konsole 'Sicherheitsrollenmanager' anzeigen".
   - Klicken Sie auf Aktionen > Sicherheitsrollenmanager.
   - Klicken Sie mit der rechten Maustaste auf die zu konfigurierende Sicherheitsrolle und klicken Sie anschließend auf Sicherheitsrollenmanager.

So greifen Sie von einem bestimmten Ordner aus auf den Sicherheitsrollenmanager zu

1. Öffnen Sie in der Symantec Management Console eine Ansicht, die den Ordner enthält, für den Sie Sicherheitsberechtigungen festlegen möchten.
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner und klicken Sie anschließend auf Sicherheit.

Besitznahme über Ordner oder Elemente

Außerdem können Sie auch mit Hilfe des Sicherheitsrollenmanagers ein Element in Besitz nehmen. Dies kann erforderlich sein, wenn versehentlich Berechtigungen für ein Element entfernt wurden und der Besitzer keinen Zugriff mehr darauf hat. Durch die Besitzergreifung können Sie die nötigen Berechtigungen zurücksetzen und den Zugriff für den ursprünglichen Besitzer wiederherstellen.

Um einen Ordner oder ein Element in Besitz nehmen zu können, benötigen Sie das Privileg "In Besitz nehmen" sowie die Berechtigung "Vollständige Kontrolle" für den Ordner bzw. das Element. Die Rolle "Symantec Administrators" hat dieses Privileg und diese Berechtigung für alle Elemente und Ordner.

Siehe "Anpassen der Vererbungsregeln für Berechtigungen" auf Seite 109.

So nehmen Sie Ordner oder Elemente in Besitz

1. Wählen Sie im linken Teilfenster des Sicherheitsrollenmanagers den Ordner bzw. das Element aus, den/das Sie in Besitz nehmen möchten.
2. Klicken Sie im rechten Teilfenster auf Erweitert.
3. Klicken Sie im Fenster "Berechtigungen für:" *Elementname* auf In Besitz nehmen.
4. Klicken Sie auf "Änderungen speichern".
5. Klicken Sie auf "Abbrechen", um das Fenster *"Berechtigungen für: Elementname"* zu schließen.

Verwalten von Identifikationsdaten

Credential Manager stellt einen sicheren Speicherort für Benutzernamen und Kennwörter zur Verfügung. Ihre installierten Verwaltungslösungen bestimmen die Typen der Identifikationsdaten, die Credential Manager speichert.

Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.

Siehe "Credential Manager-Berechtigungen" auf Seite 531.

Der Zugriff auf Identifikationsdaten wird mit der integrierten rollenbasierten Sicherheit der Symantec Management-Plattform gesteuert.

Verwaltungslösungen erstellen gewöhnlich Identifikationsdaten, wenn sie zum Ausführen einer Aufgabe erforderlich sind. Um Identifikationsdaten manuell zu definieren, müssen Sie den verwendeten Identifikationsdatentyp und die für diesen Typ erforderlichen Informationen kennen.

Wenn Identifikationsdaten erstellt werden, hat nur der Ersteller Zugriff. Beim Bearbeiten von Identifikationsdaten können Sie das Kennwort aktualisieren und Zugriff für zusätzliche Benutzer und Gruppen gewähren.

Sie können die Identifikationsdaten auch löschen. Bevor Sie Identifikationsdaten löschen, müssen Sie sicherstellen, dass sie nicht als Teil einer aktiven Verwaltungsaufgabe erforderlich sind.

So erstellen Sie Identifikationsdaten

1. Klicken Sie in "Symantec Management Console" im Menü "Einstellungen" auf "Alle Einstellungen".
2. Klicken Sie im linken Teilfenster auf "Überwachung und Warnmeldungen > Identifikationsdateneinstellungen > Identifikationsdatenverwaltung".
3. Klicken Sie im rechten Teilfenster auf "Identifikationsdaten hinzufügen".

4 Wählen Sie im Dialogfeld "Identifikationsdaten hinzufügen" einen Identifikationsdatentyp aus und geben Sie die erforderlichen Werte an.

5 Klicken Sie auf "OK".

So bearbeiten Sie Identifikationsdaten

1 Klicken Sie in "Symantec Management Console" im Menü "Einstellungen" auf "Alle Einstellungen".

2 Klicken Sie im linken Teilfenster auf "Überwachung und Warnmeldungen > Identifikationsdateneinstellungen > Identifikationsdatenverwaltung".

3 Wählen Sie im rechten Teilfenster Identifikationsdaten aus und klicken Sie dann auf "Bearbeiten".

4 Im Dialogfeld "Identifikationsdaten bearbeiten" aktualisieren Sie die Identifikationsdaten und klicken Sie dann auf "OK".

Kapitel 5

Konfigurieren von Zeitplänen

In diesem Kapitel werden folgende Themen behandelt:

- Verwendung von Zeitplänen durch die Symantec Management-Plattform
- Komponenten eines Symantec Management-Plattform-Zeitplans
- Verwalten gemeinsam genutzter Zeitpläne
- Konfigurieren eines Zeitplans
- Anzeigen des internen Zeitplankalenders des Notification Servers

Verwendung von Zeitplänen durch die Symantec Management-Plattform

Die Symantec Management-Plattform verwendet Zeitpläne für Aufgaben und Richtlinien.

Siehe "Komponenten eines Symantec Management-Plattform-Zeitplans" auf Seite 125.

Tabelle 5-1 Zeitplanverwendung

Verwendung	Beschreibung
Planung von Serveraufgaben und Serverrichtlinien	Viele Vorgänge in der Symantec Management-Plattform werden geplant, um in regelmäßigen Abständen ausgeführt zu werden. Einige diese Vorgänge müssen häufig ausgeführt werden. Dazu gehört beispielsweise die Aktualisierung der Mitgliedschaft der Ressourcengruppen und -filter. Andere können weniger häufig ausgeführt werden, wie zum Beispiel die Bereinigung älterer Datensätze aus der CMDB. Diese Zeitpläne werden normalerweise konfiguriert, um in regelmäßigen Abständen wiederholt zu werden, und sie bleiben für unbestimmte Zeit aktiv.
Planung von Agent-Aufgaben	Zeitpläne können verwendet werden, wenn Sie Vorgänge auf verwalteten Computern ausführen möchten. Beispielsweise zum Verteilen eines Patch, um eine Sicherheitslücke in einer Anwendung zu beheben, oder die Erfassung des Inventars für Richtlinieneinhaltung. Sie würden normalerweise den Vorgang so bald wie möglich ausführen wollen und Sie würden ihn nur einmal ausführen. Sie können die Ausführung von Agent-Aufgaben wie folgt planen: ■ Sofort ■ Sofort, wenn ein Wartungsfenster offen ist ■ Nächstes Mal, wenn sich ein Benutzer beim Computer einloggt ■ Nächstes Mal, wenn der Computer gestartet wird Manchmal sollten Sie den Vorgang planen, um ihn einem bestimmten Datum und Uhrzeit auszuführen. Beispielsweise um 9 Uhr abends am nächsten Sonntag, um sicherzustellen, dass er nicht die Arbeit des Benutzers behindert. In seltenen Fällen müssen Sie möglicherweise die Wiederholung einer Aufgabe planen. Jedoch würde ein wiederholender Vorgang normalerweise als eine aufgabengestützte Richtlinie angesehen.

Verwendung	Beschreibung
Planung von Agent-Richtlinien	Eine Agent-Richtlinie ist eine Anweisung zur Verwaltung eines Computers. Beispielsweise kann eine Agent-Richtlinie folgende Schritte durchführen: ■ Verweigern der Ausführung einer Software ■ Erfordern, dass eine Software installiert wird ■ Erfordern, dass Inventarinformationen über einen Computer nicht älter als N Tage sind Damit sie korrekt funktionieren, müssen einige Agent-Richtlinien so geplant werden, dass sie in bestimmten Abständen ausgeführt werden. Beispielsweise muss eine Richtlinie zur Softwarerichtlinieneinhaltung regelmäßig prüfen, ob der Computer der Richtlinieneinhaltung entspricht und die entsprechende Reparatur durchführen, wenn dies nicht der Fall ist. Ebenso muss eine Inventarisierungsrichtlinie sicherstellen, dass die Inventardaten aktuell sind. Diese Zeitpläne sind normalerweise wiederkehrende Zeitpläne mit einer möglichen Wiederholung während des Arbeitstages. Die Ausführung von Agent-Richtlinien wird häufig geplant, wenn der Computer gestartet wird oder sich ein Benutzer einloggt. Wenn Sie diese Zeitpläne einrichten, müssen Sie auch beachten, wie den Wartungsfenstern entsprechen, die auf den verwalteten Computern konfiguriert wurden. Siehe "Konfigurieren der globalen Agent-Einstellungen" auf Seite 290. Siehe "Konfigurieren der spezifischen Einstellungen" auf Seite 290.
Planung von Agent-Wartungsfenstern	Ein Wartungsfenster-Zeitplan ist im Wesentlichen ein wiederkehrender Zeitplan mit einer Dauer. Sie brauchen Wartungsfenster nicht mit Computerstart, Benutzeranmeldung oder anderen Ereignisse zu planen. Für Wartungsfenster ist keine Wiederholung während des Arbeitstages erforderlich. Siehe "Konfigurieren von Wartungsfensterrichtlinien" auf Seite 292.

Komponenten eines Symantec Management-Plattform-Zeitplans

Mit Symantec Management-Plattform-Zeitplänen können Sie einmalige und sich wiederholende Vorgänge auf dem Notification Server-Computer und den verwalteten Computern zu den angegebenen Zeiten ausführen, ohne manuell Eingreifen zu müssen. Beispielsweise müssen Ressourcenfilter häufig aktualisiert werden, die CMDB muss regelmäßig bereinigt werden und Pakete müssen in geeigneten Abständen aktualisiert werden. Alle diese Aufgaben sollten geplant werden, um zu Zeiten ausgeführt zu werden, an denen sie für Ihr Unternehmen erforderlich sind.

Siehe "Verwendung von Zeitplänen durch die Symantec Management-Plattform" auf Seite 123.

Symantec Management-Plattform benutzt zwei Typen von Zeitplänen:

Gemeinsam genutzt	Diese werden auf Notification Server als gemeinsam genutzte Elemente definiert, die für jeden geplanten Vorgang verfügbar sind. Siehe "Verwalten gemeinsam genutzter Zeitpläne" auf Seite 128.
Benutzerdefiniert	Diese werden unabhängig innerhalb jeder Aufgabe, Richtlinie oder Regel konfiguriert, die geplant wird. Sie können nicht mit anderen Aufgaben, Richtlinien oder Regeln gemeinsam genutzt werden.

Tabelle 5-2 Komponenten eines Zeitplans

Komponente	Beschreibung
Aktiver Zeitraum und Zeitzone	Der aktive Zeitraum und die Zeitzone definieren den Zeitraum, innerhalb dessen ein Zeitplan auftreten kann. Alle Zeitpläne, Auslöser und Modifizierer haben folgende Eigenschaften: ■ Zeitzone Die Zeitzone, in der die Ausführung der Aufgabe geplant wird. Die Zeitzone kann lokal, Server oder UTC sein. ■ Startdatum Das Datum und die Uhrzeit, zu der der aktive Zeitraum des Zeitplans anfängt. Ein Zeitplan kann nicht vor seinem Startdatum ausgelöst werden. ■ Enddatum Das Datum und die Uhrzeit, zu der der aktive Zeitraum des Zeitplans endet. Wenn kein Enddatum angegeben wird, bleibt der Zeitplan auf unbestimmte Zeit aktiv. Ein Zeitplan kann nicht nach seinem Enddatum ausgelöst werden. Ein Zeitplan kann nicht außerhalb seines aktiven Zeitraums ausgeführt werden. Dies gilt selbst dann, wenn der Zeitplan innerhalb seines aktiven Zeitraums ausgelöst wurde, aber das Ausführen zu dieser Zeit durch einen Modifikator verhindert wurde.

Komponente	Beschreibung
Auslöser	Ein Auslöser ist ein Ereignis, das den Zeitplan veranlasst, aktiv zu werden. Ein Auslöser kann ein spezifischer Zeitpunkt und ein Datum oder ein Ereignis, wie z.B. die Anmeldung eines Benutzers an einem Computer sein. Auslöser steuern, wann der Zeitplan und die Wiederholungen ausgeführt werden. Wenn ein Zeitplan mehrere Auslöser enthält, wird er jedes Mal ausgeführt, wenn einer seiner Auslöser auftritt. Zeitplanauslöser können folgende Eigenschaften haben: ■ Genau Bestimmt die Vorgehensweise, wenn eine geplante Aufgabe nicht zu der genauen Zeit ausgeführt werden kann, an der sie geplant ist. Ist der Wert dieser Eigenschaft "Wahr", wird die geplante Aufgabe zur genauen Zeit oder überhaupt nicht ausgeführt. Wenn die Bedingungen nicht zulassen, dass die Aufgabe zur genauen geplanten Zeit ausgeführt werden kann, wird die geplante Aufgabe nicht ausgeführt. Ist der Wert dieser Eigenschaft "Falsch", wird die geplante Aufgabe zur genauen Zeit oder so bald wie möglich ausgeführt. Beispiel: Eine Aufgabe wird jede Nacht um 2.00 Uhr ausgeführt, aber der Computer ist zu dieser Zeit immer ausgeschaltet. Mit der Einstellung "Genau" können Sie die Aufgabe zu einer beliebigen Zeit ausführen, nachdem der Computer eingeschaltet wird. Diese Eigenschaft wird auf Login, Start und andere Ereignisse sowie angegebene Zeiten angewendet. ■ Dauer Der Zeitraum, für den der Zeitplan aktiv bleibt. Die Dauer kann bis 24 Stunden betragen. ■ Wiederholung Der Abstand, in dem die Aufgabe während des aktiven Zeitraums des Zeitplans wiederholt werden sollte. Der Wiederholungsabstand kann bis 24 Stunden sein.

Komponente	Beschreibung
Modifikatoren	Modifikatoren sind zusätzliche Bedingungen, die erforderlich sind, damit der Zeitplan ausgelöst werden kann. Alle Modifikatoren gelten für alle Auslöser. ■ Nur wenn ein Benutzer eingeloggt ist Wenn der Auslöser auf einem Zielcomputer auftritt, prüft der Symantec Management-Agent auf diesem Computer, ob ein Benutzer eingeloggt ist, bevor der Zeitplan ausgeführt wird. Wenn kein Benutzer angemeldet ist, wird der Zeitplan nicht auf diesen Computer ausgeführt. ■ Nur wenn kein Benutzer eingeloggt ist Wenn der Auslöser auftritt, wird der Zielcomputer überprüft, um sicherzustellen, dass kein Benutzer angemeldet ist. Wenn ein Benutzer angemeldet ist, wird der Zeitplan nicht auf diesen Computer ausgeführt.

Verwalten gemeinsam genutzter Zeitpläne

Eine beliebige Anzahl geplanter Elemente (z.B. Richtlinien, Aufgaben oder Replikaktionsregeln) kann einen gemeinsam genutzten Zeitplan verwenden. Als Alternative zur Verwendung eines gemeinsam genutzten Zeitplans können Sie einen benutzerdefinierten Zeitplan innerhalb der Richtlinie oder der Aufgabe definieren.

Siehe "Komponenten eines Symantec Management-Plattform-Zeitplans" auf Seite 125.

Gemeinsam genutzte Zeitpläne können keine Wartungsfenster aufheben. Wenn ein geplantes Element außerhalb eines Wartungsfensters ausgeführt werden soll, müssen Sie den entsprechenden benutzerdefinierten Zeitplan konfigurieren.

Ein Satz gemeinsam genutzter Zeitpläne wird mit Symantec Management-Plattform geliefert. Sie können diese ändern, um Ihren Anforderungen zu entsprechen, aber Sie können sie nicht löschen. Beispielsweise können Sie den Geschäftszeitenzeitplan so konfigurieren, das er in regelmäßigen Abständen während der normalen Geschäftszeit ausgeführt wird. Sie können den Paketaktualisierungszeitplan so konfigurieren, dass er zu einem passenden Zeitpunkt außerhalb der Geschäftszeit ausgeführt wird. Sie können auch neue gemeinsam genutzten Zeitpläne erstellen, die erforderlich sind und löschen, wenn sie nicht mehr erforderlich sind.

Sie können jeden gemeinsam genutzten Zeitplan wie erforderlich aktivieren oder deaktivieren. Alle aktivierten gemeinsam genutzten Zeitpläne sind für jedes geplante

Element verfügbar. Wenn Sie einen gemeinsam genutzten Zeitplan deaktivieren, werden alle geplanten Elemente, die den Zeitplan verwenden, deaktiviert.

Siehe "Anzeigen des internen Zeitplankalenders des Notification Servers" auf Seite 130.

So verwalten Sie gemeinsam genutzte Zeitpläne

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Gemeinsam genutzte Zeitpläne".
2. Auf der Seite "Gemeinsam genutzte Zeitpläne" haben Sie folgende Möglichkeiten:

So fügen Sie einen neuen Zeitplan hinzu	Klicken Sie auf "Plan hinzufügen" und geben Sie dann im Zeitplan-Editor die erforderlichen Details an. Siehe "Konfigurieren eines Zeitplans" auf Seite 129.
So bearbeiten Sie einen Zeitplan	Klicken Sie auf den Zeitplannamen und geben Sie dann im Zeitplan-Editor geben Sie die erforderlichen Details an. Siehe "Konfigurieren eines Zeitplans" auf Seite 129.
So aktivieren Sie einen Zeitplan	Aktivieren Sie das entsprechende Kontrollkästchen. Wenn Sie den Zeitplan deaktivieren möchten, deaktivieren Sie das Kontrollkästchen.
So löschen Sie einen Zeitplan	Klicken Sie am rechten Ende der gewünschten Zeile auf "Löschen".
So zeigen Sie an, welche Elemente derzeit einen Zeitplan verwenden	Wählen Sie in der Dropdown-Liste "Elemente, die folgenden Zeitplan verwenden:" den gewünschten Zeitplan aus. Die Namen aller Elemente (z.B. Aufgaben, Richtlinien und Replikaktionsregeln), die den ausgewählten Zeitplan verwenden, werden im unteren Fenster angezeigt.

Konfigurieren eines Zeitplans

Mit dem Zeitplan-Editor können Sie einen Zeitplan konfigurieren, der Ihren Anforderungen entspricht.

Siehe "Komponenten eines Symantec Management-Plattform-Zeitplans" auf Seite 125.

Siehe "Verwalten gemeinsam genutzter Zeitpläne" auf Seite 128.

So konfigurieren Sie einen Zeitplan

1. Geben Sie im Fenster "Zeitplan-Editor" im Feld "Name" den Namen für den Zeitplan ein.
2. Wählen Sie unter "Aufgabe planen" die Häufigkeit oder den Auslöser aus.
3. Geben Sie auf der Registerkarte "Details" die Startzeit des Zeitplans und die Tage, Wochen oder Monate an, an denen er ausgeführt werden soll.
4. Wenn der Zeitplan für einen bestimmten Datumsbereich aktiv sein soll, geben Sie auf der Registerkarte "Erweitert" die gewünschten Start- und Enddaten an.

   Standardmäßig wird ein neuer Zeitplan aktiv, sobald er erstellt wurde (vom aktuellen Datum). Der Zeitplan bleibt aktiv (es wird kein Enddatum angegeben).
5. Wenn der Zeitplan eine Aufgabe in regelmäßigen Abständen wiederholen soll, aktivieren Sie auf der Registerkarte "Erweitert" die Option "Aufgabe wiederholen".

   Geben Sie die Häufigkeit und die Dauer an.
6. Wenn der Zeitplan mehrere Zeitpläne enthalten soll, aktivieren Sie "Mehrere Zeitpläne verwenden".
7. Für jeden zusätzlichen Zeitplan, den Sie diesem Zeitplan hinzufügen möchten, klicken Sie auf "Neu" und führen Sie die Schritte 2 bis 5 aus.
8. Klicken Sie auf "OK".

Anzeigen des internen Zeitplankalenders des Notification Servers

Sie können Notification Server-Zeitplaninformationen im internen Zeitplankalender des Notification Servers anzeigen. Zu den geplanten Elemente, die Sie im Kalender anzeigen können, gehören Aufgaben, die auf dem Notification Server ausgeführt werden, Richtlinien und Automatisierungsrichtlinien. Außerdem gehören gemeinsam genutzte Zeitpläne, Sperrzeiträume, Wartungsfenster und interne Zeitpläne für den Notification Server dazu. Symantec-Lösungen können dem Kalender zusätzliche geplante Elemente hinzufügen.

Siehe "Komponenten eines Symantec Management-Plattform-Zeitplans" auf Seite 125.

Folgende Typen der geplanten Elemente werden angezeigt:

Zeitraumelemente	Diese definieren nur eine Startzeit und werden für eine unbestimmte Zeit ausgeführt. Beispiel: Wartungsfenster, Sperrzeiträume und gemeinsam genutzte Zeitpläne.

Ereigniselemente	Diese haben eine definierte Endzeit. Beispiel: Aufgaben, Jobs, benutzerdefinierte Zeitpläne und Richtlinien. Beachten Sie, dass Richtlinien nicht immer zu den Zeiten ausgeführt werden, die im Kalender angezeigt werden. Richtlinien sind nicht so zeitgebunden wie Aufgaben, können also abhängig von Verzögerung sein. Aufgaben und Jobs werden immer zu den Zeiten aktiviert, die im Kalender gezeigt werden.

In der Kalenderansicht können Sie sehen, welche Zeitpläne für bestimmte Zeiträume, wie z.B. bestimmte Tage, Wochen oder Monate, konfiguriert werden. In der Wochen- und Monatsansicht können Sie auf einen bestimmten Tag klicken, um die Tagesansicht für diesen Tag zu öffnen.

Einige geplante Elemente verwenden gemeinsam genutzte Zeitpläne anstatt eigener Zeitpläne. Beziehungen mit gemeinsam genutzten Zeitplänen werden im linken Teilfenster in der Ansicht "Tag" dargestellt. Die geplanten Elemente sind unter dem gemeinsam genutzten Zeitplan gruppiert, auf den sie verweisen.

Mit jedem Zeitplan ist ein Symbol verbunden, das ihn mit der entsprechenden Konfigurationsseite verknüpft, wenn eine verfügbar ist. Sie können auf das Symbol klicken, um zur Konfigurationsseite zu gehen, die in einem neuen Fenster geöffnet wird. Wenn keine Konfigurationsseite für einen Zeitplan verfügbar ist, wird das Standardkalendersymbol verwendet und es ist keine Drilldown-Funktionalität gegeben.

Siehe "Verwalten gemeinsam genutzter Zeitpläne" auf Seite 128.

Siehe "Konfigurieren eines Zeitplans" auf Seite 129.

So zeigen Sie den Notification Server-Zeitplankalender an

1. Klicken Sie in "Symantec Management Console" im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster "Einstellungen > Notification Server" und klicken Sie anschließend auf "Kalender für Zeitpläne".
3. Wählen Sie auf der Seite "Kalender für Zeitpläne" in der Dropdown-Liste "Ansicht" die gewünschte Ansicht aus.

4 Wählen Sie den anzuzeigenden Zeitraum aus, indem Sie auf das entsprechende Symbol klicken:

Tag	Zeigt die Details zu allen Zeitplänen an, die ein- oder mehmals pro Tag ausgeführt werden. Die Zeitpläne werden in der Reihenfolge ihrer Startzeiten aufgelistet. Das linke Teilfenster zeigt die Zeitpläne und das rechte Teilfenster ihre Vorkommen im Kalender an. Die Tagesansicht ist die Standardansicht. Jedes Vorkommen eines Zeitraumelements wird als Raute angezeigt. Jedes Vorkommen eines Ereigniselements wird normalerweise als Balken angezeigt, aber die, die in sehr kurzen Abständen auftreten, werden als kleine Rauten angezeigt. Für bessere Übersicht auf dem Bildschirm werden Ereignisse mit einem Abstand kleiner als 15 Minuten (standardmäßig) ausgelassen. Die Hintergrundfarbe identifiziert die Geschäftsstunden, die für das Unternehmen definiert wurden.
Woche	Zeigt die Details zu allen Zeitplänen an, die weniger als einmal pro Tag aber mindestens einmal pro Woche ausgeführt werden.
Monat	Zeigt die Details zu allen Zeitplänen an, der weniger als einmal pro Woche ausgeführt werden. Zeitraumelemente werden ausgelassen und Ereigniselemente werden zu ihren Startzeiten, Endzeiten und Namen zusammengefasst.

5 Um frühere oder spätere Zeiträume anzuzeigen, klicken Sie auf "Zurück" bzw. "Weiter".

Kapitel 6

Konfigurieren von Sites und Site Servers

In diesem Kapitel werden folgende Themen behandelt:

- Info zu Site Services
- Info zur Site-Verwaltung
- Verwalten von Sites
- Verwalten von Site Servers
- Manuelles Zuweisen eines Site Server zu einer Site
- Verwalten manuell zugewiesener Agents
- Verwalten von Subnetzen
- Info zum Konfigurieren der Einstellungen für den Site Service
- Konfigurieren der Package Service-Einstellungen
- Konfigurieren der Task Service-Einstellungen

Info zu Site Services

Symantec Management-Plattform kann einige Typen von Middleware-Komponenten, z. B. Package Server, Task Server und Bootserver, bedienen. Middleware-Komponenten können auf anderen Computern als den Notification Server-Computern installiert werden. Diese Services dienen als erster Kontaktpunkt für die Symantec Management-Agents und reduzieren so die Belastung des Notification Server.

Der offizielle Name für eine Middleware-Komponente ist "Site Service". Jeder Computer, der als Host für einen Site Service fungiert, wird als Site Server bezeichnet. Auf einem Site Server kann mindestens ein Site Service installiert sein. Beispiel: Wenn Sie den Package Server-Site Service ("Package Service") auf einen Computer installieren, wird dieser Computer ein Site Server.

Site Server können Notification Server unterstützen. Site Server können die Architektur erweitern, die Verteilungseffizienz verbessern und Netzwerkbandbreiteanforderungen reduzieren.

Notification Server bearbeitet die Verteilung, Konfiguration und laufende Wartung der Site Services. Package Service, Task Service und der Boot Service beliefern die Symantec-Management Agents mit Paketen, Aufgaben und PXE-Broadcasts.

Notification Server übernimmt die folgenden Aufgaben in der Standortverwaltung:

- Bearbeitet die Verteilung auf die bzw. das Entfernen der Site Services von den Site Servern
- Stellt sicher, dass der Site Service nur auf den Computern installiert wird, die die minimalen Systemanforderungen erfüllen.

Sie verwenden die Standortverwaltung, um logische Gruppen von Endpunkten für den Lastenausgleich der Site Server zu erstellen. Beispielsweise können Sie mit mehreren Package Servern effizient Pakete an die Symantec Management-Agents verteilen. Die Package Server bearbeiten die meisten Paketverteilungsfunktionen, wodurch Notification Server entlastet wird und andere Aktivitäten durchführen kann.

Siehe "Info zur Site-Verwaltung" auf Seite 134.

Info zur Site-Verwaltung

Unter Standortwartung versteht man die Verwaltung der Standorte, Subnetze und Site Services in Ihrer Organisation. Sie können Ihre Computer entsprechend dem Standort und Subnetz verwalten, wodurch Sie Gruppen von Computern steuern und dabei den Bandbreitenverbrauch minimieren können. Ein Standort ist üblicherweise ein physischer Standort in Ihrer Organisation (beispielsweise ein bestimmtes Gebäude bzw. die Etage eines Gebäudes). Ein Subnetz ist ein Bereich logischer Adressen in Ihrem Netzwerk.

Unter normalen Betriebsbedingungen wartet jeder Package Server oder Task Server nur die Symantec Management-Agents, die innerhalb der zugewiesenen Standorte vorhanden sind. Wurde keine Standorte definiert, stehen alle Site Server für die Wartung aller Symantec Management-Agents zur Verfügung (obwohl dies nicht empfohlen ist).

Wurden keine Standorte für einen Package Server oder Task Server definiert, verwendet der Notification Server die folgenden Regeln:

- Notification Server versucht zuerst, Site Server auf demselben Subnetz zu finden, auf dem sich der anfordernde Computer befindet. Wenn Site Server gefunden werden, werden diese an den Symantec Management-Agent zurückgegeben.
- Wenn keine Site Server sich im gleichen Subnetz wie der anfordernde Computer befinden, werden alle Site Server an den Symantec Management-Agent zurückgegeben.
- Wenn keine Site Server verfügbar sind, wird der Agent an den Notification Server-Computer verwiesen.

Sie können Site Server mit Hilfe der folgenden Methoden Standorten zuweisen:

- Weisen Sie das Subnetz zu, das den Site Server für einen Standort enthält.
  Siehe "Verwalten von Subnetzen" auf Seite 142.
- Weisen Sie den Site Server einem Standort zu.
  Siehe "Manuelles Zuweisen eines Site Server zu einer Site" auf Seite 140.
- Verwenden Sie den Connector für Active Directory, um die Aufgabe durchzuführen.
  Der Connector für Active Directory überschreibt Subnetze und Standorte, die Konflikte verursachen. Beispiel: Wenn Sie Subnetze manuell einem Standort zuweisen, der in Konflikt zu dem steht, was sich im Connector für Active Directory befindet, werden die Active Directory-Informationen verwendet.

Nachdem die Liste der verfügbaren Site Server an den Symantec Management-Agent zurückgegeben wurde, wählt der Agent den am besten geeigneten Site Server.

Site Server und verwaltete Computer können über mehrere Netzwerkkarten und IP-Adressen verfügen und deshalb durch Subnetzzuweisung zu mehr als einem Standort gehören.

Siehe "Info zu Site Services" auf Seite 133.

Siehe "Verwalten von Sites" auf Seite 135.

Siehe "Verwalten von Site Servers" auf Seite 137.

Siehe "Verwalten von Subnetzen" auf Seite 142.

Verwalten von Sites

Sie müssen alle Standorte einrichten, die Sie in Ihrer Organisation benötigen. Sie können eine Standort-Importregel ausführen, um die Standortinformationen für Ihre Organisation automatisch von Active Directory zu erfassen. Sie können Standorte

auch manuell erstellen und ihnen die entsprechenden Subnetze und Site Server zuweisen.

So verwalten Sie Sites

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Site Server-Einstellungen".
2. Führen Sie einen der folgenden Schritte aus:

Neuen Standort erstellen	1. Klicken Sie im linken Teilfenster auf "Neu" > "Standort". 2. Geben Sie im Fenster "Neue Site" im Feld "Name" den neuen Namen der Site ein. 3. Wenn Sie der Site sofort Subnetze zuweisen möchten, geben Sie diese ein. 4. Klicken Sie auf "OK".
Standort ändern	1. Wählen Sie im linken Teilfenster den Standort aus, den Sie ändern möchten, und klicken Sie dann auf "Konfigurieren". 2. Wenn Sie den Namen der Site ändern möchten, geben Sie im Fenster "Site bearbeiten" im Feld "Name" einen neuen Namen ein. 3. Sie können die der Site zugewiesenen Subnetze ändern, indem Sie die entsprechenden Subnetze angeben. 4. Klicken Sie auf "OK".
Löschen einer Site	Wählen Sie im linken Teilfenster den Standort aus, den Sie löschen möchten, und klicken Sie dann auf "Löschen". Subnetze, die dem Standort zugewiesen sind, werden nicht gelöscht. Ihre Zuweisung wird aufgehoben und sie können anderen Standorten zugewiesen werden. Site Server innerhalb der betroffenen Subnetze werden erst verwendet, wenn sie einem anderen Standort zugewiesen werden.
Manuell zugewiesene Site Server aus einem Standort entfernen	Wählen Sie im linken Teilfenster unter "Site Server", den Standort aus, den Sie entfernen möchten, und klicken Sie dann auf "Löschen". Der Site Server ist davon nicht betroffen und ist weiterhin Server für andere Standorte, denen er zugewiesen ist. Diese Option gilt nur für diejenigen Site Server, die Standorten manuell zugewiesen werden. Ein Site-Server, der durch seine Subnetzmitgliedschaft zu einem Standort gehört, kann nicht von diesem Standort entfernt werden.

Subnetz aus Standort entfernen	Wählen Sie im linken Teilfenster unter "Standort" das Subnetz aus, das Sie löschen möchten, und klicken Sie dann auf "Löschen". Durch Löschen eines Subnetzes wird die Zuweisung des Subnetzes zu jedem Standort aufgehoben. Die Zuweisung aller eingeschlossenen Subnetze, die einem Standort nicht manuell zugewiesen werden, wird auch aufgehoben. Alle Site Server im Subnetz bzw. in den eingeschlossenen Subnetzen sind nicht mehr Server des Standorts. Jedoch sind sie weiterhin Server für Standorte, denen sie manuell zugewiesen werden.
Manuell zugewiesene Agents verwalten	Sie können Agents einem Standort zuweisen und alle entfernen, die Sie nicht mehr benötigen. Siehe "Verwalten manuell zugewiesener Agents" auf Seite 141.

Verwalten von Site Servers

Sie müssen alle in Ihrem Unternehmen benötigten Site Server erstellen und sie den entsprechenden Sites zuweisen. Wählen Sie zum Erstellen von Site Servers die gewünschten Computer aus und geben Sie die zu installierenden Site Services an. Sie können vorhandene Site Server auch ändern, indem Sie Site-Dienste hinzufügen oder entfernen. Notification Server stellt dann die entsprechenden Installationspakete auf den ausgewählten Computern bereit und entfernt die nicht erforderlichen. Beachten Sie, dass die Änderungen erst übernommen werden, wenn die Symantec Management-Agents auf den Zielcomputern die nächste Konfigurationsanforderung senden.

Um sicherzustellen dass die Site Services richtig installiert und konfiguriert sind, empfiehlt Symantec, die Site Services über die Symantec Management Console zu installieren.

Hinweis: Auf dem Task Server-Computer müssen IISs 6.0 bzw. IISs 7.0 sowie .NET Frameworks 3.5 aktiviert sein.

Wenn ein Site Server ausgewählt wird, zeigt die Seite "Standortdienste" Statistiken für jeden Standortdienst an, der auf ihm installiert ist. Die ausgeblendete Ansicht zeigt zusammenfassende Details an, während die erweiterte Ansicht ein Teilfenster für jeden Standortdienst mit vollständigen Details und grafischen Informationen anzeigt. Jedes Teilfenster mit Standortdiensten enthält auch einen Link zur entsprechenden Seite für die Konfiguration der globalen Einstellungen.

Die Titelleiste für jeden Standortdienst enthält ein Symbol, das seinen aktuellen Status anzeigt:

Grün	Der Dienst ist installiert und wird auf dem Site Server ausgeführt.
Gelb	Der Dienst ist derzeit nicht auf dem Site Server installiert.
Orange	Der Dienst befindet sich im Warnzustand.
Rot	Der Dienst ist nicht verwendbar. Ein Paket ist ungültig.

So verwalten Sie Site Server

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Site Server-Einstellungen".
2. Führen Sie einen der folgenden Schritte aus:

Site Server erstellen

1. Klicken Sie im linken Teilfenster auf "Neu" > "Site Server".
2. Wählen Sie im Dialogfeld "Ausgewählte Computer" die Computer aus, die den Site Services hinzugefügt werden sollen, und klicken Sie auf "OK".

   Die Liste im linken Teilfenster enthält alle Computer, die zur Verfügung stehen, um als Site Server verwendet zu werden. Wenn Sie die Symantec Management-Plattform installieren, müssen Sie dem System zum Füllen dieser Liste einige Minuten Zeit lassen.
3. Aktivieren Sie im Dialogfeld "Dienste hinzufügen/entfernen" die entsprechenden Kontrollkästchen, um die Site Services auszuwählen, die auf jedem Site Server installiert werden sollen, und klicken Sie auf "Weiter".

   Unter jedem Computer sind die jeweils verfügbaren Services aufgelistet. Die Kontrollkästchen für Diensttypen, die auf einem bestimmten Computer nicht installiert werden können, werden grau angezeigt. Sie können die Liste nach Site Servern oder nach Diensten gruppieren. Durch Auswählen eines übergeordneten Knotens in der Liste werden all seine untergeordneten Elemente ausgewählt.

   Wenn ein Kontrollkästchen bereits aktiviert ist, weist dies darauf hin, dass der entsprechende Site Service bereits installiert ist. Wenn Sie ihn entfernen möchten, deaktivieren Sie das Kontrollkästchen.
4. Klicken Sie auf "OK".

Ändern eines Site Server

1. Vergewissern Sie sich, dass in der Tabelle "Detaillierte Informationen" die Ansicht "Site Server" ausgewählt ist, und wählen Sie den gewünschten Site Server aus.
2. Klicken Sie auf das Symbol "Bearbeiten".

Site Server manuell einem Standort zuweisen

Wählen Sie den entsprechenden Site Server aus, und klicken Sie dann auf "Standort zuweisen".

Siehe "Manuelles Zuweisen eines Site Server zu einer Site" auf Seite 140.

Entfernen eines manuell zugewiesenen Site Server aus einer Site	Wählen Sie im linken Teilfenster unter "Site Server", den Standort aus, den Sie entfernen möchten, und klicken Sie dann auf "Löschen". Der Site Server ist davon nicht betroffen und ist weiterhin Server für andere Standorte, denen er zugewiesen ist. Diese Option gilt nur für diejenigen Site Server, die Standorten manuell zugewiesen werden. Ein Site-Server, der durch seine Subnetzmitgliedschaft zu einem Standort gehört, kann nicht von diesem Standort entfernt werden.

Video: Weitere Informationen zum Rollout eines Task Server finden Sie unter Rollout eines Task Server mit ITMS: Video - Teil 1, Windows XP und Rollout eines Task Server mit ITMS: Video - Teil 2, Windows Server 2008 R2 auf Symantec Connect.

Manuelles Zuweisen eines Site Server zu einer Site

Site Server funktionieren automatisch als Server des Standorts, dem ihr übergeordnetes Subnetz zugewiesen ist. Site Server können mehrere NICs/IPs haben und in mehr als einem Subnetz sein. Folglich können sie zu mehr als einem Standort gehören. Sie können jeden Site Server auch einem oder mehreren anderen Standorten manuell zuweisen. Die Spalte "Manuell zugewiesen" in der Tabelle mit den ausführlichen Informationen gibt an, ob der Site Server dem Standort manuell zugewiesen ist.

Siehe "Verwalten von Site Servers" auf Seite 137.

Wenn Sie einen Site Server einem Standort manuell zuweisen, wird nur der Site Server dem ausgewählten Standort zugewiesen. Das Subnetz, zu dem der Site Server gehört, ist davon nicht betroffen.

So weisen Sie einen Site Server manuell einem Standort zu

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Site Server-Einstellungen".
2. Vergewissern Sie sich, dass in der Tabelle "Detaillierte Informationen" die Ansicht "Site Server" ausgewählt ist, und wählen Sie den gewünschten Site Server aus.
3. Klicken Sie auf "Standort zuweisen".
4. Wählen Sie im Fenster "Standort auswählen" den Standort aus, dem Sie den Site Server zuweisen möchten.
5. Klicken Sie auf "OK".

Verwalten manuell zugewiesener Agents

Ein manuell zugewiesener Agent ist ein Computer, der manuell einem Standort statt über sein Subnetz zugewiesen wurde. Es empfiehlt sich, bestimmte Computer manuell einem Standort zuzuweisen, um von der Subnetzanweisung abzukommen. Sie können neue Agents manuell einem Standort zuweisen, indem Sie die relevanten Ressourcenziele dem Standort zuweisen. Sie können alle Agents entfernen, die nicht am Standort sein sollen, indem Sie die entsprechenden Ressourcenziele einem anderen Standort zuweisen.

Hinweis: Wenn der manuell zugewiesene Agent ein Task Server ist, tritt die Änderung erst in Kraft, wenn Sie Symantec Management-Agent auf dem Computer zurücksetzen. Eine Möglichkeit zum Zurücksetzen des Symantec-Management Agent ist im Symantec Management Agent auf der Registerkarte "Aufgabenstatus" auf "Agent zurücksetzen" zu klicken. Eine andere Methode ist die Ausführung der Aufgabe "Task Agent zurücksetzen" auf dem Computer

So verwalten Sie zugewiesene Agents manuell

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Site Server-Einstellungen".
2. Erweitern Sie im linken Teilfenster den Standort oder den Site Server, den Sie ändern möchten, und klicken Sie anschließend auf "Manuell zugewiesene Agents".
3. Führen Sie auf der Seite "Manuell zugewiesene Agents" einen der folgenden Schritte aus:

Manuell zugewiesene Agents einem Standort hinzufügen	Klicken Sie auf "Neu" und wählen Sie anschließend im Fenster "Gruppe auswählen" die entsprechenden Ressourcenziele aus oder erstellen sie. Siehe "Auswählen benannter Ressourcenziele" auf Seite 403.
Manuell zugewiesene Agents einem anderen Standort neu zuweisen	Diese Option steht nur unter dem Knoten "Standort", nicht jedoch unter dem Knoten "Site Services" zur Verfügung. Wählen Sie die entsprechenden Ressourcenziele aus, und klicken Sie anschließend auf "Standort zuweisen". Wählen Sie im Fenster "Standort auswählen" den entsprechenden Standort aus, und klicken Sie anschließend auf "OK".
Manuell zugewiesene Agents aus Site entfernen	Wählen Sie die entsprechenden Ressourcenziele aus, und klicken Sie anschließend auf "Löschen".

Verwalten von Subnetzen

Sie müssen alle Subnetze in Ihrer Organisation erstellen und sie den entsprechenden Standorten zuweisen. Sie können Subnetze neu synchronisieren, falls erforderlich, und alle Subnetze löschen, die nicht mehr existieren.

Subnetze können aus den Grundinventardaten ermittelt werden, die aus Active Directory importiert oder manuell hinzugefügt wurden. Sie können eine Subnetz-Importregel ausführen, um die Subnetz-Informationen automatisch aus Active Directory zu erfassen.

Bei Subnetzen folgt als Suffix immer die Anzahl der in der Netzwerkmaske festgelegten Bits (z. B. 192.168.0.0/24). Die Subnetze werden immer in einer hierarchischen Verzeichnisstruktur dargestellt. Die Bereiche der Ressourcen werden festgelegt, so dass Sie nur die Subnetze sehen können, die Ressourcen enthalten, zu denen Sie Zugriff haben.

Sie müssen jedes Subnetz dem entsprechenden Standort zuweisen. Standardmäßig werden alle eingeschlossenen Subnetze (ein Subnetz, dessen IP-Bereich vollständig in einem anderen Subnetz enthalten ist) automatisch demselben Standort zugewiesen. Jedoch können Sie das Einbeziehen von Subnetzen manuell aufheben, indem Sie ein eingeschlossenes Subnetz explizit einem anderen Standort zuweisen. Standardmäßig werden eingeschlossene Subnetze unter ihren übergeordneten Subnetzen im linken Teilfenster angezeigt. Wenn jedoch ein Subnetz manuell einer anderen als seiner übergeordneten Site zugewiesen wird, wird es unter dieser Site angezeigt.

Alle Site Server auf einem Subnetz werden automatisch demselben Standort wie das Subnetz zugewiesen. Diese Anweisung wird nicht unterbrochen, wenn Sie einen Site Server manuell einem anderen Standort zuweisen. Ein Site Server kann einer beliebigen Anzahl von Standorten manuell zugewiesen werden, und zwar zusätzlich zum Standort, für den er durch seine Subnetzuweisung als Server fungiert.

So verwalten Sie Subnetze

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Site Server-Einstellungen".
2. Führen Sie einen der folgenden Schritte aus:

Neues Subnetz erstellen

1. Klicken Sie im linken Teilfenster auf "Neu" > "Subnetz".
2. Geben Sie im Dialogfeld "Neues Subnetz" die Subnetznetzwerkadresse, die Subnetzmaske sowie die Site, der dieses Subnetz zugewiesen werden soll, an und klicken Sie dann auf "OK".

   Wenn Sie die **Tabulatortaste** drücken oder in dieses Feld klicken, nachdem Sie die Subnetz-Netzwerkadresse eingegeben haben, wird automatisch eine Maske entsprechend den folgenden Regeln ausgewählt:

   - Das System überprüft das erste Oktett einer IPv4-Adresse, um festzulegen, ob es ein Subnetz der Klasse A, B oder C ist. Es wählt dann die entsprechende Standardmaske aus.
   - Wenn die Netzwerkadresse spezifischer (d.h. ein weiteres Oktett ungleich Null) ist als für diese Klasse zulässig, dann werden zusätzliche Byte in der Standardmaske festgelegt.
   - Wenn die Adresse nicht in einem erkannten Format vorliegt oder das letzte Oktett ungleich Null ist, wird keine Standardmaske vorgeschlagen.

   Sie können die Standardmaske manuell bearbeiten, falls erforderlich. Beachten Sie, dass nach dem manuellen Bearbeiten der Subnetzmaske ein Aktualisieren der Netzwerkadresse im Feld "Subnetz" die Maske nicht mehr aktualisiert.

Löschen eines Subnetzes

Erweitern Sie im linken Teilfenster "Site-Verwaltung > Subnetze" das zu löschende Subnetz aus und klicken auf dann "Entf".

Wenn Sie ein Subnetz löschen, das Sie manuell erstellt haben, ist es dauerhaft gelöscht. Jedoch werden alle Subnetze wiederhergestellt, die vom Grundinventar oder von Active Directory importiert wurden, sobald die Daten aktualisiert werden.

Subnetz einem Standort zuweisen

1. Erweitern Sie im linken Teilfenster den Eintrag "Site-Verwaltung" und klicken Sie dann auf "Subnetze".
2. Wählen Sie im rechten Teilfenster das entsprechende Subnetz aus und klicken Sie dann auf "Site zuweisen".
3. Wählen Sie im Dialogfeld "Site auswählen" die Site aus, der das Subnetz zugewiesen werden soll, und klicken Sie dann auf "OK".

Erneutes Synchronisieren von Subnetzen	1 Erweitern Sie im linken Teilfenster den Eintrag "Site-Verwaltung" und klicken Sie dann auf "Subnetze". 2 Klicken Sie im rechten Teilfenster auf "Subnetze neu synchronisieren". Notification Server verweist auf die CMDB für aktuelle Subnetzinformationen. Es liest die Subnetzzuweisung, die in den Ergebnissen des neuesten Agent Inventory-Scans enthalten ist. Notification Server aktualisiert anschließend die Liste der Subnetze dementsprechend.

Info zum Konfigurieren der Einstellungen für den Site Service

Die Einstellungen für den Site Service sind normalerweise globale Standardeinstellungen. Alle Änderungen, die Sie an den Einstellungen für einen bestimmten Typ von Site Service vornehmen, werden für alle Site Services dieses Typs übernommen. Einige Typen von Site Services verfügen mitunter über Einstellungen, die individuell für Dienste konfiguriert werden können. Dann werden die Standardvorgaben überschrieben. Beispielsweise kann jeder Package Server als "Eingeschränkt" oder "Uneingeschränkt" konfiguriert werden, wodurch die Standardeinstellung aufgehoben wird.

Sie können die globalen Einstellungen für jeden Site Service anzeigen und ändern. Jeder Site Service (z. B. Package Server) hat eine Seite, auf der die zugehörigen globalen Einstellungen bearbeitet werden können.

Im linken Teilfenster werden unter dem Site Server alle installierten Dienste angegeben. Die entsprechende Seite enthält eine Übersicht über die Dienste des Site Servers. Dieses Fenster ist standardmäßig eingeblendet, nicht ausgeblendet wie für Statistiken auf der Seite "Site Server". Über den Link "Einstellungen ändern" können Sie die globalen Einstellungen für diesen Diensttyp bearbeiten.

Bei vielen Diensten sind die hier angezeigten Übersichtsinformationen unter Umständen mit den erweiterbaren auf der Seite "Site Server" identisch. Bei Bedarf können Dienste mithilfe der Symantec Management-Plattform in diesem Zusammenhang aber mit anderen Steuerelementen versehen werden. Gibt es beispielsweise eine ganze Seite mit verfügbaren Daten, wird diese auf der Seite für den Site Service angezeigt. Ein reduzierter Datensatz wird auf der Seite "Site Server" angezeigt.

Siehe "Konfigurieren der Package Service-Einstellungen" auf Seite 146.

Siehe "Konfigurieren der Task Service-Einstellungen" auf Seite 146.

Weitere Informationen zum Überwachungsdienst finden Sie im *Benutzerhandbuch zu Monitor Solution*.

Konfigurieren der Package Service-Einstellungen

Konfigurieren Sie die globalen Package Service-Einstellungen. Diese Einstellungen werden auf alle Package Services angewendet, die auf Site Servern in Ihrer Symantec Management-Plattform installiert sind.

So konfigurieren Sie Package Service-Einstellungen

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Site Server-Einstellungen".
2. Im linken Teilfenster erweitern Sie "Einstellungen > Package Service" und klicken Sie auf "Package Service-Einstellungen".
3. Konfigurieren Sie auf der Seite "Package Service-Einstellungen" die entsprechenden Einstellungen:

So stellen Sie die globalen Package Service-Einstellungen ein	Nehmen Sie im Fenster Globale Package Service-Einstellungen die notwendigen Änderungen vor. Für weitere Informationen klicken Sie auf die Seite und drücken Sie dann **"F1"**.
So richten Sie uneingeschränkte Package Server ein	Richten Sie im Fenster "Eingeschränkte Package Server-Auswahl" die einzelnen Package Server ein, indem Sie das Kontrollkästchen "Eingeschränkt" je nach Wunsch aktivieren oder deaktivieren. Mithilfe der Dropdown-Liste für den Standort können Sie zusammengefasste Informationen über alle Package Server an bestimmten oder allen Standorten anzeigen.

4. Klicken Sie auf "Änderungen speichern".

Konfigurieren der Task Service-Einstellungen

Sie können Task Service-Einstellungen auf die Task Server anwenden, die Computer, Benutzer oder Ressourcen verwenden. Notification Server wendet diese Einstellungen auf die ausgewählten Task Services an, die auf den Site Servern in Ihrer Umgebung installiert sind.

Siehe "Informationen zu Task Management " auf Seite 426.

Siehe "Sequenzieren von Aufgaben" auf Seite 436.

So konfigurieren Sie Task Service-Einstellungen

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Site Server-Einstellungen".
2. Erweitern Sie im linken Teilfenster "Einstellungen > Task Service > Einstellungen" und klicken Sie anschließend auf "Task Service-Einstellungen".
3. Konfigurieren Sie auf der Seite "Task Service-Einstellungen" die gewünschten Einstellungen.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.
4. Klicken Sie im Fenster "Gilt für" auf "Zuordnen zu", um die Computer, Benutzer oder Ressourcen auszuwählen, auf die diese Task Service-Einstellungen angewendet werden.

   Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

   Diese Einstellungen werden auf die Task Services angewendet, die diese Computer, Benutzer oder Ressourcen verwenden.
5. Klicken Sie auf "Änderungen speichern".

Kapitel 7

Konfigurieren der Package Server für Linux

In diesem Kapitel werden folgende Themen behandelt:

- Info zu Package Server für Linux
- Info zur Integration von Apache Web Server mit Package Server für Linux
- Info zur Erkennung von Apache Web Server
- Konfigurationsanforderungen für Package Server und Apache Web Server
- Konfigurationsanforderungen von HTTPS und HTTP
- Package Server-Konfigurationsbeispiel, dass das Haupt-Webverzeichnis für Package Server-Links verwendet
- Package Server-Konfigurationsbeispiel unter Verwendung eines Alias für Package Server-Links

Info zu Package Server für Linux

Um einen Linux-Computer als Package Server festzulegen stellen Sie sicher, dass der Computer die folgende Software ausführt:

- Symantec Management-Agent für UNIX, Linux und Mac
  Dieser Agent war vorher als Altiris Agent für UNIX und Linux bekannt. Symantec Management Agent für UNIX, Linux und Mac kann auf einem verwalteten Computer ausgeführt werden. Dieser Agent muss der Version des Agents entsprechen, der auf dem Notification Server-Computer in der Symantec Management-Plattform installiert wird. Wenn der Agent auf dem verwalteten Computer älter als der Agent auf dem Notification Server ist, führen Sie ein

Upgrade durch. Nach der Durchführung des Upgrade kann aus dem verwalteten Computer ein Package Server werden.

- Apache Web Server Version 2.0 oder 2.2
  Siehe "Info zur Integration von Apache Web Server mit Package Server für Linux" auf Seite 149.

Die folgenden Serverplattformen werden unterstützt:

- Red Hat Enterprise Linux Server 5
- Red Hat Enterprise Linux Server 6
- SUSE Linux Enterprise Server 10
- SUSE Linux Enterprise Server 11 SP1, 11 SP2

Package Server für Linux unterstützt alternative Download-Speicherorte. Die Pfade für alternative Speicherorte werden automatisch von Windows zu UNIX konvertiert, wenn Sie den abschließenden Schrägstrich einschließen. Wenn Sie beispielsweise Patch Management Solution installiert haben, können Sie die Richtlinien- und Paketeinstellungen bei der Verteilung von Patches ändern. Klicken Sie in der Symantec Management Console unter "Einstellungen > Alle Einstellungen > Software > Patch-Management" auf eine Seite mit Händlereinstellungen, beispielsweise auf "Red Hat-Einstellungen > Red Hat-Patch – Reparatureinstellungen". Wenn Sie auf die Registerkarte "Richtlinien- und Paketeinstellungen" klicken, wird die Seite "Reparatureinstellungen" für das ausgewählte Produkt angezeigt. Hier können Sie "Alternatives Download-Verzeichnis auf Package Server verwenden" aktivieren. Wenn Sie den alternativen Downloadort eingeben, müssen Sie den vollen Windows-Pfad verwenden. Schließen Sie den Windows-Pfad in dieser und in ähnlichen Instanzen mit einem abschließenden Schrägstrich ab um sicherzustellen, dass er richtig in einen UNIX-Pfad konvertiert wird.

Richtig: "C:\path\"	Der abschließende Schrägstrich bedeutet, dass der Windows-Pfad richtig in "/path/" konvertiert wurde.
Falsch: "C:\path"	Wenn Sie den abschließenden Schrägstrich auslassen, wird der Windows-Pfad falsch konvertiert.

Info zur Integration von Apache Web Server mit Package Server für Linux

Sie integrieren Package Server für Linux mit dem Apache Web Server, um Pakete und Paket-Snapshots dem Symantec Management Agent bereitzustellen. Die

Snapshots werden vom Notification Server auf den Symantec Management Agent auf allen unterstützten Plattformen durch HTTP URL heruntergeladen.

Siehe "Info zu Package Server für Linux" auf Seite 148.

Die Pakete und die Paket-Snapshots werden immer in Package Server-Verzeichnisse heruntergeladen. Die einzigen auf dem Apache Web Server erstellten Dateien sind Verzeichnisse, symbolische Links und .htaccess-Dateien. Symbolische Links werden zu den Paketdateien und den Snapshot-Dateien erstellt. Die .htaccess-Dateien sichern die Paketdateien mit Kennwörtern.

Wenn aus einem Linuxcomputer ein Package Server wird, versucht der Agent auf diesem Computer zwei HTTP-Hauptfreigaben zu erstellen.

Diese Freigaben werden im virtuellen Internet-Speicherplatz des Apache Web Servers wie folgt erstellt:

- /Altiris/PS/Snapshots
- /Altiris/PS/Packages Note /Altiris/PS
  Dies zweite Verzeichnis wird, falls erforderlich, erstellt.

Die Manifest-Datei des Pakets wird nicht verwendet, wenn ein Package Server für Linux ein Paket zur Verteilung herunterlädt. Die Ausnahme besteht bei einem Paket, das sich im gleichen Verzeichnis für den Package Server für Linux und der Software Delivery befindet. Alle Paketdatei-Berechtigungen erlauben den Zugriff der Apache Web Server-Clients. Dieser Zugriff wird gewöhnlich durch 0x744 ausgeführt.

Abhängig von der spezifischen Konfiguration des Apache Web Servers werden die Verzeichnisse auf der Stammebene im Internet-Verzeichnis erstellt. Ein Beispiel dazu ist "/var/www/html" auf einem typischen Linux-Red Hat-System. Der Package Server-Agent liest die Apache Web Server-Konfigurationsdatei, um diesen Speicherort festzulegen.

Siehe "Info zur Erkennung von Apache Web Server" auf Seite 150.

Bei der Auswahl dieser Option können Sie festlegen, dass die Verzeichnisse vom Package Server an einem alternativen Speicherort erstellt werden. Verwenden Sie eine Apache Web Server-Aliasrichtlinie, um ein separates Verzeichnis festzulegen.

Siehe "Konfigurationsanforderungen für Package Server und Apache Web Server" auf Seite 152.

Siehe "Konfigurationsanforderungen von HTTPS und HTTP" auf Seite 153.

Info zur Erkennung von Apache Web Server

Sie können Apache Web Server automatisch oder manuell erkennen.

Siehe "Info zur Integration von Apache Web Server mit Package Server für Linux" auf Seite 149.

Siehe "Konfigurationsanforderungen für Package Server und Apache Web Server" auf Seite 152.

Wenn Sie die automatische Erkennung auswählen, sucht Symantec Management Agent nach den Programmen Apache HTTPD oder HTTPD2 in den folgenden Verzeichnissen:

- /bin:/usr/bin:/sbin:/usr/sbin:/usr/lbin:/usr/etc:/etc:/usr/bsd:/usr/local/bin:/usr/contrib/bin/
- System PATH-Variable
- /opt/apache/bin:/usr/apache/bin:/usr/apache2/bin:/usr/local/apache/bin:/usr/local/apache2/bin:/usr/local/bin:/opt/freeware/apache/bin:/opt/freeware/apache2/bin:/opt/freeware/apache/sbin:/opt/hpws/apache/bin:/opt/apache2:/usr/local/apache+php

Wenn beide HTTPD und HTTPD2 gefunden wurden, dann werden Apache 2.0 und Apache 2.2 installiert.

Zusätzlich wird die Datei verwendet, die einem laufenden Prozess entspricht, wenn beide ausführbaren Dateien gefunden werden. Die Standarddatei ist HTTPD2.

Wenn der Apache Web Server nicht automatisch erkannt werden kann, müssen Sie ihn möglicherweise manuell erkennen. Der Apache Web Server wird möglicherweise nicht automatisch erkannt, wenn die ausführbare Datei umbenannt wird. Wenn mehrere Installationen ausgeführt wurden, könnte der falsche Apache Web Server erkannt werden. In diesen Situationen sollten Sie den Speicherort des Apache Web Servers manuell angeben.

Um den Speicherort des Apache Web Servers manuell anzugeben, bearbeiten Sie den Abschnitt [httpd-Integration] in der Datei "client.conf" im Agent. In diesem Abschnitt sollten Sie die Einstellung "apache_exe_location" bearbeiten.

Wenn die Apache Web Server-Datei gefunden wurde, wird sie zur Festlegung des Standardorts der Apache Web Server-Konfigurationsdatei verwendet. Die Konfigurationsdatei wird benötigt um festzulegen, ob die Apache Web Server-Installation als Package Server geeignet ist. Die Konfigurationsdatei lässt das Installationsprogramm auch die Einstellungen festlegen, die auf den Package Server anwendbar sind. Die anwendbaren Einstellungen umfassen die verwendeten Ports oder die mögliche Server SSL-Aktivierung.

Wenn Symantec Management Agent für UNIX, Linux und Mac die Apache Web Server-Konfigurationsdatei nicht finden kann, wird danach in den folgenden Speicherorten gesucht:

- /etc/httpd/conf

- /etc/httpd/2.0/conf

Sie können als Alternative zur automatischen Erkennung den Abschnitt "[Httpd-Integration]" in der Datei "client.conf" des Symantec Management Agents für UNIX-, Linux- und Mac bearbeiten. Wenn Sie die Datei bearbeiten, geben Sie die "apache_config_location" an. Jede Einstellungsänderung wird als Standard verwendet.

Sie können die Option "Apache Web Server "- f" während der Installation verwenden, um die Konfigurationsdatei von seinem Standardort zu verschieben. Wenn Sie die Datei verschieben, müssen Sie den Speicherort unter "apache_config_location" angeben. Package Server für Linux unterstützt keine "mod_perl generierte httpd.conf"-Dateien.

Konfigurationsanforderungen für Package Server und Apache Web Server

Damit der Package Server für Linux mit dem Apache Web Server funktioniert, müssen bestimmte Voraussetzungen erfüllt sein. Wenn diese Voraussetzungen erfüllt wurden, sendet Symantec Management Agent für UNIX, Linux und Mac die Apache-HTTP-Server-Rolle. Durch diese Rolle kann der Computer dann als Package Server für Linux verwendet werden.

Siehe "Info zur Erkennung von Apache Web Server" auf Seite 150.

Die Konfigurationsanforderungen lauten wie folgt

- Apache Web Server Version 2.0 oder 2.2 installiert.
- Der Package Server für Linux verwendet nur den Haupt-Apache- oder nur den Standard Apache Web Server.
  Alle weiteren Abschnitte des virtuellen Host in der Apache Web Server-Konfiguration, werden mit den folgenden Ausnahmen ignoriert:
  - Die globalen Einstellungen und der virtuelle _default_ Host werden für die grundlegenden Servereinstellungen eingelesen.
  - Der erste virtuelle Host, der einen SSL-Server definiert, gilt als der Haupt-SSL-Server. Seine Einstellungen werden für die Integrierung verwendet und alle weiteren virtuellen SSL-Hosts werden ignoriert.
- Für den Internet-Speicherplatzspeicherort des Apache Web Servers, in dem die Package Server-Daten und Verzeichnisse erstellt werden, müssen folgende Optionen aktivieren werden:
  - "FollowSymLinks"
  - "AllowOverride"

Der Internet-Speicherplatzspeicherort des Apache Web Servers muss auch über anonymes HTTP zugänglich sein. Der Speicherort ist das virtuelle Verzeichnis " /Altiris/PS/".
Siehe "Konfigurationsanforderungen von HTTPS und HTTP" auf Seite 153.

- Wenn HTTP und HTTPS für Apache Web Server festgelegt werden, wird der HTTPS-Server verwendet.
- Nicht standardmäßige Ports werden erkannt und verwendet, der Haupt-Apache Web Server aber muss über den Hostnamen des Computers zugänglich sein. Die Richtlinie "Listen" für den Hauptserver muss vor allen anderen "Port" -Anweisungen und "Listen"-Richtlinien in der Konfigurationsdatei stehen.
- Der Apache Web Server muss ausgeführt werden.
- Es werden keine komprimierten Module mit dem Apache Web Server verwendet. Diese Anforderung besteht, da die Paketverteilung diese Module nicht unterstützt.
- Sie müssen Symantec Management Agent für UNIX, Linux und Mac möglicherweise neu starten, nachdem Sie an der Datei "httpd.conf" Änderungen vorgenommen haben. Die Dateien werden möglicherweise erst nach dem Neustart des Agent übernommen.

Konfigurationsanforderungen von HTTPS und HTTP

Symantec Management Agent für UNIX-, Linux- und Mac verwendet den aktuell verfügbaren Apache Web Server. Es kann entweder HTTP oder HTTPS verwendet werden.

Siehe "Konfigurationsanforderungen für Package Server und Apache Web Server" auf Seite 152.

Wenn der Apache Web Server beide Webserverarten unterstützt, verwendet der Package Server für Linux HTTPS. Die Integrierung von SSL durch HTTPS ist die Standardoption, da sie die sicherste Methode darstellt. Wenn Sie den HTTP-Server verwenden möchten, können Sie die Einstellung [httpd-Integration] integrate_with ändern.

Tabelle 7-1 Empfohlene Ansätze für das Installieren von Apache Web Server zur Unterstützung von Package Servern für UNIX und Linux

Option	Beschreibung
Installieren Sie eine Paketversion von Apache Web Server. Linux ist für einen verteilten Apache Web Server am geeignetsten.	Diese Installation enthält die ausführbaren Dateien und die exe-Dateien des technischen Supports in "/usr/sbin" oder "/usr/bin".

Option	Beschreibung
Installieren Sie das Apache Web Server-Paket im empfohlenen Speicherort.	Ein Beispiel eines geeigneten Standardorts lautet "/usr/local oder /opt".
Belassen Sie das Konfigurationsverzeichnis an seinem Standardort. Mit dieser Anforderung können Sie sicherstellen, dass Symantec Management Agent für UNIX, Linux und Mac den Apache Web Server und die Konfigurationsdatei leicht erkennen kann. Wenn Sie das Konfigurationsverzeichnis nicht verschieben, sind keine manuellen Einstellungen erforderlich.	Das Standard-Konfigurationsverzeichnis ist der Speicherort, der in der ".exe-Datei" oder "/etc/httpd/conf" kompiliert wurde.

Wenn Sie die Apache Web Server-Konfigurationsdateien ändern, während Symantec Management Agent ausgeführt wird, werden Daten nach einer kurzen Zeit zum Notification Server geschickt. Nachdem die Apache Web Server-Rollendaten zum Notification Server geschickt wurden, wird aus dem Computer ein potenzieller Package Server. Wenn Sie diesen Prozess beschleunigen möchten, sollten Sie die ausführbare Datei "aex-sendbasicinventory" manuell ausführen. Führen Sie die ausführbare Datei in der Eingabeaufforderung auf dem Clientcomputer aus, auf den die Package Server-Installation abzielt. Aktualisieren Sie Notification Server mit den Änderungen.

Es sind zwei Konfigurationsbeispiele verfügbar.

Siehe "Package Server-Konfigurationsbeispiel, dass das Haupt-Webverzeichnis für Package Server-Links verwendet" auf Seite 154.

Siehe "Package Server-Konfigurationsbeispiel unter Verwendung eines Alias für Package Server-Links" auf Seite 157.

Package Server-Konfigurationsbeispiel, dass das Haupt-Webverzeichnis für Package Server-Links verwendet

Diese Konfiguration erfordert im Allgemeinen eine minimale Änderung an der sofort einsatzbereiten oder standardmäßigen Apache Web Server-Installation. In dieser Konfiguration wird ein virtuelles Verzeichnis namens "/Altiris/PS" automatisch unter dem Apache HTML-Hauptverzeichnis erstellt.

Siehe "Konfigurationsanforderungen von HTTPS und HTTP" auf Seite 153.

Die Beispielkonfiguration enthält die folgenden Verzeichnisse:

- Snapshots
- Pakete

Es werden symbolische Links in diesen Verzeichnissen zu jedem gemeinsam genutzten Paket erstellt. Die Pakete selbst werden im Verzeichnis des Package Server-Agent "VAR" gespeichert.

Diese Konfiguration umfasst einen HTTP- und einen HTTPS Apache Server. Der Package Server verwendet den HTTPS-Server, wenn er verfügbar ist. Der HTTPS-Server stellt eine weitaus sichere Betriebsumgebung zur Verfügung und ermöglicht die Verwendung von Paket-Zugriffsberechtigungen.

Es werden mehrere Konfigurationsdateiprüfungen durchgeführt. Die in diesem Abschnitt aufgelisteten Konfigurationsdateien sind Beispieldateien. Ein Beispiel ist die Standardinstallation des Apache Web Servers als Teil einer älteren Red Hat Linux-Distribution.

Die "Prüfnummer 1; "Listen"-Anweisung" lautet wie folgt:

```
...## Wenn SSL zur Verfpgung steht, müssen auch der ## Standard
HTTP-Port (siehe oben) und der HTTPS-Port überwacht werden ##
<IfDefine HAVE_SSL> Listen 80 Listen 443 Listen 10.10.10.10:8080
</IfDefine>...
```

Stellen Sie sicher, dass die "Listen"-Anweisung für jeden der Hauptserver die erste "Listen"-Anweisung seines Typs in der Konfigurationsdatei ist. Die HTTP- und HTTPS-Hauptserver sollten als erste beiden "Listen"-Anweisungen aufgeführt sein.

Sie sollten die IP entfernen oder sicherstellen, dass der Hostname zu der gleichen IP, die dem Notification Server übermittelt wurde, aufgelöst wird.

Die "Prüfnummer 2; Hauptverzeichnisoptionen" lautet wie folgt:

```
...

# DocumentRoot: Das Verzeichnis, aus dem Ihre Notification
Server-Referenz 62 bedient wird

# documents. Standardmäßig werden alle Anfragen aus diesem Verzeichnis
entnommen, außer

# symbolische Links und Aliasnamen, sie werden möglicherweise
verwendet, um auf andere Verzeichnisse zu verweisen. DocumentRoot
"/var/www/html" ...

# Dieser Eintrag sollte auf den festgelegten "DocumentRoot" geändert
werden.

#<Directory "/var/www/html">
```

```
# Kann möglicherweise auch "Keine", "Alle" oder jede andere
Kombination von "Indexen" sein.

# "Includes", "FollowSymLinks", "ExecCGI", oder "MultiViews".

# Beachten Sie, dass "MultiViews" *ausdrücklich* --- "Optionen alle"
benannt werden muss

# keine Übergabe.

Options Indexes FollowSymLinks

# Legt fest, welche Optionen die .htaccess-Dateien in den
Verzeichnissen

# übergehen können. Kann auch "Alle" oder jede andere Kombination
von "Options", "FileInfo",

# "AuthConfig", und "Limit" AllowOverride AuthConfig sein

# Legt fest, wer Daten von diesem Server erhalten darf.

Order allow,deny

Allow from all

</Directory>

...
```

Suchen Sie den <"Verzeichnis"> -Knoten für das Verzeichnis "DocumentRoot" und stellen Sie sicher, dass die folgenden Optionen aktiviert sind:

- "FollowSymLinks"
- "AllowOverride AuthConfig" oder "Allow override All"

Die "Prüfnummer 3; Überprüfen des SSL Host" lautet wie folgt:

```
## SSL Virtual Host-Kontext

<VirtualHost _default_:443>

# Allgemeine Installation des virtueller Host

DocumentRoot "/var/www/html"

ErrorLog logs/error_log

TransferLog logs/access_log Notification Server Reference 63

# SSL Engine-Switch:

# SSL für diesen virtuellen Host aktivieren/deaktivieren.

SSLEngine on
```

...

Stellen Sie sicher, dass der virtuelle _default_ SSH-Host den richtigen Port aufweist. Der Port sollte dem ersten SSH "Listen"-Port entsprechen. Stellen Sie sicher, dass das "DocumentRoot" des virtuellen Host dem "DocumentRoot" des Hauptservers entspricht.

Das "DocumentRoot" des Host kann sich vom "DocumentRoot" des Hauptservers unterscheiden. Das "DocumentRoot" des Host muss einen <"Verzeichnis"> -Knoten besitzen, der mit den gleichen Optionen wie in Prüfnummer 2 angegeben, konfiguriert ist.

Package Server-Konfigurationsbeispiel unter Verwendung eines Alias für Package Server-Links

Betreiben Sie das virtuelle Verzeichnis von Package Server für Linux komplett vom Apache Web Server-Verzeichnis getrennt. Folgen Sie diesem Konfigurationsbeispiel, um sie separat zu betreiben. Dieses Konfigurationsbeispiel trennt alle symbolischen Links vom Apache Web Server-Hauptverzeichnis. Es stellt sicher, dass die Optionen "FollowSymLinks" nicht im Hauptverzeichnis erforderlich sind.

Siehe "Konfigurationsanforderungen von HTTPS und HTTP" auf Seite 153.

Es wird ein Alias in der Apache Web Server-Konfigurationsdatei verwendet, um das virtuelle Verzeichnis /Altiris/ PS zu trennen. Der Package Server für Linux erkennt diesen Alias automatisch und erstellt die erforderlichen Unterverzeichnisse im richtigen Verzeichnis.

Die Unterverzeichnisse sind folgende:

- Pakete
- Snapshots

Die tatsächlichen Pakete werden in das Verzeichnis VAR des Agent heruntergeladen.

Die in diesem Abschnitt verwendeten Konfigurationsdateien sind Beispieldateien. Ein Beispiel ist die Standardinstallation des Apache Web Servers als Teil einer älteren Red Hat Linux-Distribution.

Die "Prüfnummer 1; "Listen"-Anweisung" lautet wie folgt:

```
... ##, Wenn SSL zur Verfügung gestellt wird, muss der

## Standard HTTP-Port (siehe oben) und der HTTPS-Port überwacht werden

##

<IfDefine HAVE_SSL>
```

```
Listen 80

Listen 443

Listen 10.10.10.10:8080

</IfDefine>

...
```

Stellen Sie sicher, dass die "Listen"-Anweisung für jeden der Hauptserver die erste "Listen"-Anweisung seines Typs in der Konfigurationsdatei ist. Die HTTP- und HTTPS-Hauptserver sollten als erste beiden "Listen"-Anweisungen aufgeführt sein.

Sie sollten die IP entfernen oder sicherstellen, dass der Hostname zu der gleichen IP, die dem Notification Server übermittelt wurde, aufgelöst wird. Verwenden Sie andere Port-Nummern als 80 oder 443. Der Package Server für Linux erkennt die Ports. Es wird jedoch immer der erste "Listen"-Port aus der Apache Web Server-Konfigurationsdatei verwendet.

Die "Prüfnummer 2; "Erstellen"-Alias und Pseudonymverzeichnisoptionen" lautet wie folgt:

```
...

# Aliases: Fügen Sie hier soviele Alias hinzu, wie benötigt werden
(keine Einschränkung). Das Format lautet

# Alias fakename realname

#

<IfModule mod_alias.c>

...

Alias /Altiris/PS /var/altiris/www/ps

<Directory /var/altiris/www/ps >

Options FollowSymLinks

AllowOverride All

</Directory> </IfModule>

# End of aliases.
```

Sie sollten diese Schritte in der folgenden Reihenfolge durchführen:

- Erstellen Sie die Aliasanweisung und den <"Verzeichnis"> -Knoten für das Zielverzeichnis des Alias.
- Stellen Sie sicher, dass die folgenden Optionen für dieses Verzeichnis festgelegt werden:

- "FollowSymLinks"
- "AllowOverride AuthConfig" oder "Allow override All"

- Erstellen Sie das Zielverzeichnis.
- Erstellen Sie die richtigen Berechtigungen für das Zielverzeichnis um sicherzustellen, dass Dateien von den Apache Web Server-Clients von diesem Verzeichnis heruntergeladen werden können.
- Speichern Sie eine Textdatei zum Testen dieses Verzeichnisses. Navigieren Sie dann zu einer URL wie beispielsweise "http://your.server.name/Altiris/PS/testfile.txt". In diesem Beispiel ist "your.server.name" Ihr eigener Servername und "testfile.txt" der Name der erstellten Textdatei.

Die "Prüfnummer 3; Überprüfen des SSL Host" lautet wie folgt:

```
...

## SSL Virtual Host-Kontext

<VirtualHost _default_:443>

# Allgemeine Installation des virtueller Host

DocumentRoot "/var/www/html"

ErrorLog logs/error_log

TransferLog logs/access_log

# SSL Engine-Switch:

# SSL für diesen virtuellen Host aktivieren/deaktivieren.

SSLEngine on

...
```

Stellen Sie sicher, dass der virtuelle _default_ SSH-Host den richtigen Port aufweist. Es sollte dem ersten SSH "Listen-"Port entsprechen. Stellen Sie sicher, dass "DocumentRoot" dem "DocumentRoot" des Hauptservers entspricht.

Kapitel 8

Konfigurieren der Hierarchie

In diesem Kapitel werden folgende Themen behandelt:

- Info zur Notification Server-Hierarchie
- Hierarchieanforderungen
- Implementieren der Notification Server-Hierarchie

Info zur Notification Server-Hierarchie

Die Hierarchie ist eine Technologie, die entwickelt wurde, um die Gesamtbetriebskosten (TCO) für die Verwaltung der Symantec-Software und -Lösungen auf mehreren Notification Servern zu reduzieren. Die Hierarchiefunktion reduziert die Gesamtbetriebskosten (TCO), indem sie das Notification Server-System mit zentralen Verwaltungsfunktionen ergänzt.

Siehe "Hierarchieanforderungen" auf Seite 162.

Siehe "Implementieren der Notification Server-Hierarchie" auf Seite 163.

Die Hierarchiefunktion definiert den Informationsfluss auf mehreren Notification Servern in einem Unternehmen. Wenn Sie mehrere Notification Server haben, können Sie die Hierarchie verwenden, um Sammlungen von Notification Servern zu definieren, die allgemeine Konfigurationseinstellungen und -daten gemeinsam nutzen. Die Hierarchie kann alle Änderungen verteilen und synchronisieren, die an den gemeinsam genutzten Konfigurationseinstellungen und -daten vorgenommen werden. Mithilfe der Hierarchiefunktion können Sie Ihre Symantec-Lösungen auf mehreren Notification Servern von einem zentralen Standort verwalten.

Einige Lösungen wie beispielsweise "Inventory Solution", "Patch Management Solution" und "Software Management Solution" werden für die Teilnahme an der

Hierarchie eingerichtet. Informationen zu einer bestimmten Lösung finden Sie in der zugehörigen Dokumentation.

Im Zusammenhang mit Hierarchien wird Replikation verwendet, um gemeinsam genutzte Objekte und Daten zwischen Notification Servern innerhalb der gleichen hierarchischen Struktur zu kopieren und zu synchronisieren. In geplanten Abständen synchronisiert jeder Server innerhalb einer Hierarchie Objekte und Daten mit seinen unmittelbar übergeordneten und untergeordneten Elementen.

Siehe "Info zu Replikation und Replikationsregeln" auf Seite 180.

Eine Hierarchietopologie definiert die Beziehungen zwischen Notification Servers, die wiederum steuert, wie die Synchronisierung zwischen benachbarten Knoten erfolgt.

Es gelten folgende Regeln:

- Jeder Notification Server kann entweder kein oder ein übergeordnetes Element haben.
- Jeder Notification Server kann entweder kein oder mehrere untergeordnete Elemente haben.

In der Hierarchie sind Objekte und Daten auf die Replikation in bekannten Richtungen beschränkt, somit ist die Synchronisierung voraussagbar und skalierbar. Da in der Hierarchie jedes Objekt oder jeder Datensatz nur in einer Richtung repliziert wird, ist die Konfliktverwaltung einfach und die Quelle erhält immer Priorität.

Tabelle 8-1 Objekte, die zwischen Notification Servern synchronisiert werden können

Objekt	Beschreibung
Konfigurations- und Managementelemente	Richtlinien, Aufgaben, Filter und Berichte werden eine Hierarchie weiter unten repliziert. Siehe "Informationen zu ausgeführten Aufgaben in der Hierarchie" auf Seite 433.
Sicherheitseinstellungen	Sicherheitsrollen, Privilegien und Berechtigungen werden in einer Hierarchie abwärts repliziert.
Ressourcen	Ressourceninformationen, wie beispielsweise Computer, Benutzer, Sites und ihre zugeordneten Datenklassen werden in einer Hierarchie aufwärts oder abwärts repliziert.
Pakete	Pakete, die Softwareressourcen zugeordnet sind, und Datenklassen, die Paketen zugeordnet sind, werden in einer Hierarchie abwärts repliziert.

Objekt	Beschreibung
Ereignisse	Ereignisklassen, wie beispielsweise Software Delivery-Ausführung, werden in einer Hierarchie aufwärts oder abwärts repliziert.

Hinweis: Einige Symantec-Lösungen erstellen benutzerdefinierte Replikationsregeln, um sicherzustellen, dass bestimmte Elemente immer synchronisiert werden.

Hierarchieanforderungen

Wenn Sie Konfigurationseinstellungen und Daten auf anderen Notification Server-Computern gemeinsam nutzen möchten, müssen Sie den Notification Server-Computer zuerst einer Hierarchie hinzufügen. Da Notification Server-Computer lokal verwaltet werden können, muss jeder Notification Server-Computer einer Hierarchie mit den entsprechenden Zugriffsidentifikationsdaten hinzugefügt oder aus ihr entfernt werden. Der Symantec-Administrator, der die Topologie verwaltet, fügt Notification Server an anderen Standorten einer Hierarchie per Remote-Zugriff hinzu.

Siehe "Info zur Notification Server-Hierarchie" auf Seite 160.

Siehe "Implementieren der Notification Server-Hierarchie" auf Seite 163.

Anforderungen für das Konfigurieren von Hierarchien:

- Routing des Netzwerkverkehrs muss zwischen benachbarten Notification Server-Computern in der Hierarchie möglich sein.
- HTTP/HTTPS-Datenverkehr muss zwischen benachbarten Notification Server-Computern innerhalb der Hierarchie zulässig sein.
- Wenn Sie selbstsignierte Zertifikate für Notification Server-Computer verwenden, stellen Sie sicher, dass ein Vertrauensverhältnis zwischen diesen Computern besteht. Installieren Sie dazu in der Microsoft Management Console, im Speicher "Zertifikate (lokaler Computer)" Zertifikate manuell auf "Vertrauenswürdige Stammzertifizierungsstelle".
- Es muss Vertrauensbeziehungen zwischen benachbarten Notification Server-Computern in der Hierarchie geben, oder die Identifikationsdaten für die privilegierten Konten müssen bekannt sein.
- Jeder Notification Server-Computer muss den Namen und die Netzwerkadresse benachbarter Notification Server-Computer innerhalb der Hierarchie auflösen können.

- Es muss genug Bandbreite zwischen Notification Server-Standorten vorhanden sein, damit die Paket- und Datenreplikation unterstützt werden kann.
  Die erforderliche Bandbreite und Hardware hängt von der Größe der Hierarchietopologie und den replizierten Daten ab.
- Es muss ein Standort für jeden Notification Server-Computer vorhanden sein, und dieser muss das Subnetz einschließen, das den Notification Server enthält. Der Standort muss auch einen Package Server enthalten (ein Site Server, auf dem der Paketdienst ausgeführt wird), auf dem sich der Notification Server befindet.
  Siehe "Info zu Site Services" auf Seite 133.

Implementieren der Notification Server-Hierarchie

Damit Sie Konfigurationseinstellungen und Daten mit mehreren Notification Servers gemeinsam nutzen oder anfordern können, müssen Sie den Notification Server-Computer einer Hierarchie hinzufügen und die notwendigen Replikationsregeln konfigurieren.

Tabelle 8-2 Implementieren der Notification Server-Hierarchie

Schritt	Aktion	Beschreibung
Schritt 1	Erstellen Sie die entsprechenden hierarchischen Beziehungen zwischen Notification Servern.	Sie erstellen ein Hierarchie durch Erstellen einer Reihe von Übergeordnet/Untergeordnet- und Untergeordnet/Übergeordnet-Beziehungen, die die Notification Server-Computer in Ihrem System verbinden. Siehe "Erstellen und Verwalten hierarchischer Beziehungen" auf Seite 164. Siehe "Einrichten einer Hierarchiebeziehung zwischen zwei Notification Server-Computern" auf Seite 168.
Schritt 2	Erstellen und aktivieren Sie die entsprechenden Replikationsregeln zur Angabe der Daten, die durch die Hierarchie repliziert werden sollen.	Die Hierarchiereplikation von Ressourcen und Ereignissen wird mit Hilfe von Replikationsregeln konfiguriert. Diese Regeln definieren die Daten, die auf anderen Notification Servers repliziert werden sollen. Siehe "Konfigurieren der Hierarchiereplikation und Hierarchiereplikationsregeln" auf Seite 170. Wenn Sie eine benutzerdefinierte Hierarchiereplikation für Konfigurations- und Verwaltungselemente einrichten möchten, nehmen Sie die entsprechenden Einstellungen vor. Siehe "Einrichten der benutzerdefinierten Hierarchiereplikation" auf Seite 173.

Schritt	Aktion	Beschreibung
Schritt 3	(Optional) Führen Sie die manuellen Replikationsaufgaben aus.	Die in einer Hierarchie enthaltenen Notification Server-Computer werden normalerweise nach dem Replikationszeitplan synchronisiert, der in den Replikationsregeln eingerichtet wurde. Sie können bei Bedarf den Differenzial-Replikationszeitplan für den Notification Server manuell übergehen und die Hierarchiereplikationsregeln sofort auslösen. Siehe "Übergehen des Differenzial-Replikationszeitplans für Hierarchien" auf Seite 174. Sie können auch ausgewählte Daten direkt aus einem Notification Server manuell auf alle ihm untergeordneten Notification Server replizieren, ohne dies in einer Replikationsregel aufzunehmen. Manuelle Replikation ist eine einmalige, sofort stattfindende Replikation. Sie benötigen die Leseberechtigung, damit die Replikation auf über den Kontextmenüeintrag "Jetzt replizieren" durchgeführt werden kann. Siehe "Manuelles Replizieren ausgewählter Daten" auf Seite 175.
Schritt 4	(Optional) Einrichten von Hierarchieautomatisierungsrichtlinien.	Automatisierungsrichtlinien für die Hierarchie senden E-Mail-Benachrichtigungen, wenn bestimmte Ereignisse in der Hierarchie auftreten. Siehe "Einrichten einer Hierarchieautomatisierungsrichtlinie" auf Seite 176.
Schritt 5	Ausführen eines Hierarchieberichts.	Sie können einen Bericht auf einem beliebigen Notification Server in der Hierarchie ausführen, um Daten aus dessen CMDB zu extrahieren. Aktualisieren der Zusammenfassungsdaten vor dem Ausführen eines Hierarchieberichts. Siehe "Ausführen eines Hierarchieberichts" auf Seite 177. Siehe "Aktualisieren von Übersichtsdaten" auf Seite 178.

Siehe "Info zur Notification Server-Hierarchie" auf Seite 160.

Siehe "Hierarchieanforderungen" auf Seite 162.

Erstellen und Verwalten hierarchischer Beziehungen

Sie erstellen ein Hierarchie durch Erstellen einer Reihe von Übergeordnet/Untergerordnet- und Untergeordnet/Übergerordnet-Beziehungen, die die Notification Server-Computer in Ihrem System verbinden. Sie können Ihren Notification Server (den Notification Server, bei dem Sie angemeldet sind, auch remote) als untergeordneten oder übergeordneten Server eines bestehenden remote Notification Server zu einer Hierarchie hinzufügen.

Sie können Ihren Notification Server (den Notification Server, bei dem Sie angemeldet sind, auch remote) als untergeordneten oder übergeordneten Server eines bestehenden Remote Notification Server zu einer Hierarchie hinzufügen. Um eine hierarchische Beziehung zu erstellen, benötigen Sie auf beiden Computern ein Symantec-Administratorkonto (oder ein Konto mit gleichwertigen Privilegien). Um Notification Server-Computer einer Hierarchie hinzuzufügen oder daraus zu entfernen, benötigen Sie auf dem Notification Server-Computer, auf dem die Aktion ausgeführt wird, das Privileg "Hierarchietopologie verwalten".

Sie können den Notification Server-Computer mit Hilfe der Symantec Management Console anzeigen und konfigurieren. Wenn Sie der Hierarchieadministrator sind, können Sie nur die über- und untergeordneten Elemente (bis in alle Stufen hinunter) Ihres Notification Server sehen.

Beachten Sie, dass alle ausgeführten Aktionen auf Ihrem Notification Server basieren. Durch das Klicken mit der rechten Maustaste auf einen Notification Server wird kein Remote-Login für einen Remote Notification Server durchgeführt. Ein Kontextmenü mit den Aktionen, die Sie auf diesem Server ausführen können, wird geöffnet; es ist nicht dasselbe für lokale und Remote-Computer. Für den lokalen Server ist ein vollständiger Satz von Aktionen vorhanden, aber für Remote-Server gibt es nur einen beschränkten Satz. Aktionen wie die Extrahierung von Berichten werden auf der entsprechenden Datenbank ausgeführt.

Die Aktionen, die Sie für die Hierarchie ausführen können, hängen von Ihrem Notification Server ab, d. h. von dem Computer, auf dem Sie angemeldet sind. Wenn Sie auf einem Remote Notification Server-Computer über das Privileg "Hierarchie verwalten" verfügen, können Sie sich auf diesem Computer per Fernzugriff einloggen. Dann können Sie die Symantec Management Console öffnen und die Hierarchiekonfiguration für diesen Computer vornehmen.

Sie können die Hierarchiereplikation auf bestimmten Notification Servern zu jeder Zeit aktivieren oder deaktivieren. Sie können diese Funktion zum Beispiel dazu verwenden, die Hierarchiereplikation temporär zu deaktivieren, während Verwaltungsaufgaben wie Installationen, Upgrades oder Deinstallationen von Lösungen vorgenommen werden. Eine Deaktivierung der Replikation auf einem Notification Server hat keinen Einfluss auf den Replikationszeitplan der anderen Notification Server in der Hierarchie. Es werden jedoch keine Daten an den deaktivierten Computer weitergegeben, d.h., die Replikation nach unten hört beim übergeordneten Computer auf und die Replikation nach oben hört bei den untergeordneten Computern auf.

Ein farbiges Symbol auf der Seite "Hierarchieverwaltung" gibt an, dass es Hierarchie-Warnmeldungen gibt. Im Folgenden werden die möglichen Farben und die jeweiligen Warnstatus angezeigt:

Gelb	Niedriger Warnstatus.

Orange	Mittlerer Warnstatus.
Rot	Kritischer Warnstatus. Falls Sie zum Beispiel versuchen, dieselben Daten vom selben Notification Server nach oben und nach unten in der Hierarchie zu replizieren, wird eine kritische Warnmeldung erstellt. Daten sollten nur in eine Richtung repliziert werden. Wenn auf dem über- oder dem untergeordneten Notification Server dieselben Hierarchie-Replikationsregeln implementiert sind, könnte es zu Datenkonflikten kommen.

Diese Aufgabe stellt einen Schritt im Prozess der Implementierung der Notification Server-Hierarchie dar.

Siehe "Implementieren der Notification Server-Hierarchie" auf Seite 163.

So erstellen und verwalten Sie hierarchische Beziehungen

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Hierarchie".
2. Wählen Sie auf der Seite "Hierarchieverwaltung" auf der Registerkarte "Topologie" in der Dropdown-Liste "Ansicht" die Option "Diagramm", um die Hierarchie als Grafik anzuzeigen.

   Verwenden Sie die Ansicht "Raster" nur zum Kopieren von Daten auf die Zwischenablage. Sie enthält Daten, die in der Ansicht "Diagramm" nicht angezeigt werden.

3 Führen Sie eine der folgenden Aufgaben durch:

Hinzufügen eines neuen Notification Servers zu einer Hierarchie	Siehe "Einrichten einer Hierarchiebeziehung zwischen zwei Notification Server-Computern" auf Seite 168.
Ändern einer hierarchischen Beziehung zwischen zwei Notification Servern	Siehe "Einrichten einer Hierarchiebeziehung zwischen zwei Notification Server-Computern" auf Seite 168.
Entfernen eines Notification Servers aus der Hierarchie	Klicken Sie mit der rechten Maustaste auf den zu entfernenden Notification Server-Computer und klicken Sie dann auf "Entfernen".
Aktivieren oder Deaktivieren der Hierarchiereplikation	Sie sollten die Teilnahme an der Hierarchie deaktivieren, wenn Sie Wartungsarbeiten an einem Notification Server vornehmen. Klicken Sie mit der rechten Maustaste auf den Notification Server-Computer, auf dem Sie die Hierarchiereplikation aktivieren bzw. deaktivieren möchten, und klicken Sie auf "Replikation aktivieren" bzw. "Replikation deaktivieren. Das Deaktivieren der Hierarchiereplikation wirkt sich nur auf den Zeitplan der Hierarchiereplikation aus. Sie hat keinen Einfluss auf Standalone-Replikationen, die für oder von einem anderen Notification Server eingerichtet wurden. Die manuelle Synchronisierung der Hierarchie ändert diese Einstellung nicht, sondern überschreibt sie, um eine einmalige Replikation der entsprechenden Elemente auszuführen.
Manuelles Überschreiben des Zeitplans für die Hierarchiereplikation für einen Notification Server	Siehe "Übergehen des Differenzial-Replikationszeitplans für Hierarchien" auf Seite 174.
Ausführen eines Hierarchieberichts	Siehe "Ausführen eines Hierarchieberichts" auf Seite 177.

4 Klicken Sie auf "Änderungen speichern".

Siehe "Info zur Notification Server-Hierarchie" auf Seite 160.

Siehe "Hierarchieanforderungen" auf Seite 162.

Video: Weitere Informationen zum Einrichten einer Hierarchie finden Sie in dem Video Erstellen einer Hierarchie in der IT Management Suite auf Symantec Connect.

Einrichten einer Hierarchiebeziehung zwischen zwei Notification Server-Computern

Sie können eine Hierarchiebeziehung (entweder übergeordnete oder untergeordnete Elemente) zwischen Ihrem Notification Server-Computer und einem standortfernen Notification Server-Computer einrichten. Sie müssen den Namen, die URL (die alle nicht standardmäßigen Portkonfigurationen oder HTTPS enthalten muss) und Zugriffsdetails des standortfernen Notification Server-Computers angeben. Sie müssen auch die Zugriffsdetails Ihres lokalen Notification Server-Computers angeben. Standardmäßig staffelt der Zeitplan für die Hierarchiereplikation die Replizierung zwischen jedem Notification Server-Computer-Paar. Sie können den Replikationszeitplan Ihren Anforderungen entsprechend ändern, aber Sie sollten sicherstellen, dass die Staffelung der Replikation aufrechterhalten wird.

Auf beiden Notification Server-Computern muss ein Package Server innerhalb ihrer jeweiligen Standorte verfügbar sein. Der Package Server ist aus Leistungsgründen erforderlich. Sie können keine Hierarchiebeziehung zwischen zwei Notification Server-Computern erstellen, wenn auf einem davon kein Package Server verfügbar ist.

Die Notification Server-Anwendungsidentifikationsdaten sollten beständig sein und nicht wie einige Benutzerkontokennwörter regelmäßig geändert werden. Falls das Kennwort des Notification Server-Computers nicht mehr gültig ist, wird eine Meldung in der Konsole angezeigt. In der Meldung werden Sie aufgefordert, das ASConfig-Kommandozeilenprogramm zu verwenden, um die notwendigen Updates vorzunehmen.

Diese Aufgabe ist ein Schritt beim Implementieren der Notification Server-Hierarchie.

Siehe "Implementieren der Notification Server-Hierarchie" auf Seite 163.

So richten Sie eine Hierarchiebeziehung zwischen zwei Notification Server-Computern ein

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server Management > Hierarchie".
2. Klicken Sie auf der Seite "Hierarchieverwaltung" auf der Registerkarte "Topologie" mit der rechten Maustaste auf Ihren Notification Server, und klicken Sie anschließend auf die entsprechende Option:
   - "Hinzufügen" > "Übergeordnetes Element"
   - "Hinzufügen" > "Untergeordnetes Element"

3 Geben Sie im "Assistent zum Hinzufügen von Hierarchieknoten" auf der Seite "Notification Server" den Namen, die URL und die Identifikationsdaten für den Remote-Notification Server ein.

   Die Identifikationsdaten müssen ein Symantec-Administratorkonto oder gleichwertiges Konto auf dem standortfernen Notification Server-Computer sein.

4 Klicken Sie auf "Erweitert".

5 Geben Sie im Dialogfeld "Identifikationsdateneinstellung zurückgeben" das Konto des Symantec-Administrators (oder ein gleichwertiges Konto) an, das der Remote-Notification Server verwendet, um mit dem lokalen Notification Server zu kommunizieren, und klicken Sie auf "OK".

6 Klicken Sie im Assistent zum Hinzufügen von Hierarchieknoten auf "Weiter".

7 Richten Sie auf der Seite "Replikationszeitpläne" die differenziellen und vollständigen Replikationszeitpläne ein, aktivieren Sie diejenigen, die auf dem Notification Server-Computer genutzt werden sollen und klicken Sie auf "Weiter".

   Standardmäßig ist nur der Differenzial-Replikationszeitplan aktiviert. Die vollständige Replikation wird nur selten genutzt, weil sie den Notification Server-Computer schwer belastet. Sie können sie jedoch bei Bedarf aktivieren. Sie sollten die Replikation zu den Zeiten planen, die nicht mit Replikationszeitplänen auf anderen Notification Server-Computern in der Hierarchie kollidieren.

   Siehe "Verwalten gemeinsam genutzter Zeitpläne" auf Seite 128.

   Siehe "Konfigurieren eines Zeitplans" auf Seite 129.

8 Überprüfen Sie auf der Seite "Einstellungen bestätigen", ob die Einstellungen korrekt sind, und klicken Sie anschließend auf "Fertig stellen".

   Der lokale Notification Server verwendet die angegebenen Informationen, um den standortfernen Notification Server-Computer zu finden, zu überprüfen und die entsprechende Hierarchiebeziehung mit ihm einzurichten.

   Wenn der standortferne Notification Server-Computer nicht über einen Package Server innerhalb seines Standorts verfügt, schlägt die Überprüfung fehl und die Hierarchiebeziehung kann nicht aufgebaut werden.

Siehe "Info zur Notification Server-Hierarchie" auf Seite 160.

Siehe "Hierarchieanforderungen" auf Seite 162.

Konfigurieren der Hierarchiereplikation und Hierarchiereplikationsregeln

Die Hierarchiereplikation legt fest, was in der Hierarchie repliziert wird. Sie hat keine Auswirkung auf die unabhängige Replikation, die zwischen zwei Notification Servern eingerichtet werden kann.

Wenn Sie einen Notification Server einer Hierarchie hinzufügen, können Sie festlegen, was an den übergeordneten Notification Server und was an beliebige untergeordnete Notification Server repliziert werden soll. Standardmäßig wird alles repliziert (volle Replikation), das übermäßige Bandbreite verbrauchen kann. Sie sollten die Hierarchiereplikation auf jedem Notification Server den Anforderungen Ihres Unternehmens entsprechend konfigurieren.

Hinweis: Replikation wird zwischen zwei Notification Servers, auf denen verschiedene Versionen von IT Management Suite installiert ist, nicht unterstützt. Beispiel: Sie können Daten nicht von einem 7.0-Server auf einen 7.1-Server replizieren.

Daten, die von einem übergeordneten Notification Server nach unten repliziert wird, haben Priorität und überschreiben die entsprechenden Daten auf den untergeordneten Servern. Die replizierten Konfigurations- und Verwaltungselemente, die von einem übergeordneten Server empfangen werden, sind in der Regel schreibgeschützt, sodass sie nicht geändert werden können. Die Schreibschutzeinstellung gewährleistet, dass eine unveränderte Abwärtsreplikation in der Hierarchie stattfindet. Wenn Hinzufügungen von replizierten Elementen auf untergeordneten Servern gestattet werden sollen, müssen Sie die entsprechenden Elemente auf dem Notification Server-Computere entsperren, auf dem sie erstellt wurden. Sie können z. B. gestatten, dass bestimmte Richtlinien auf den untergeordneten Notification Servern aktiviert oder deaktiviert werden können.

Die Hierarchiereplikation von Ressourcen und Ereignissen wird mit Hilfe von Replikationsregeln konfiguriert. Diese Regeln definieren die Daten, die auf anderen Notification Servers repliziert werden sollen. Jede Regel repliziert die angegebenen Daten in nur einer Richtung, entweder auf den übergeordneten oder nach unten auf den untergeordneten Notification Server. Wenn Sie zwei Regeln einrichten, die über den gleichen Ressourcentyp verfügen, der in beide Richtungen repliziert wird, wird eine Warnmeldung angezeigt und die Replizierungsregeln werden nicht ausgeführt.

Sie können Ressourcenziele in eine Ressourcenreplizierungsregel einschließen. Ressourcen mit Bereichsfestlegung gelten für den Inhalt (Ressourcen) der Ziele, die repliziert werden. Aus diesem Grund hängen die replizierten Ressourcen vom Eigentümer des Ressourcenziels ab. Der Notification Server-Administrator kann

festlegen, dass Ressourcenziele in ihrem aktuellen Status (im Besitz eines anderen Benutzers mit dem entsprechenden Berechtigungsumfang) repliziert werden. Er kann sich auch die Ziele zuweisen, diese mit Administratorumfang speichern (schließt normalerweise mehr Ressourcen ein) und dann in diesem Status replizieren. Alle aktuellen Elemente eines Ressourcenziels werden repliziert. Das eigentliche Ressourcenzielelement wird im Hintergrund als abhängiges Objekt repliziert. Wenn eine Replikationsregel, die auf ein Ressourcenziel zutrifft, beispielsweise im übergeordneten Element erstellt wird, wird das Ressourcenziel als abhängiges Element repliziert, wenn die Replikationsregel selbst durch die Hierarchie nach unten repliziert wird.

Hierarchie verfügt über zwei Replikationsmodi:

Differenziell	Repliziert Objekte und Daten, die seit der letzten Replikation geändert wurden. Dieser Modus ist standardmäßig aktiviert und verringert die Auslastung und die Bandbreite, die von der Hierarchie benötigt wird.
Abgeschlossen	Repliziert alle Objekte und Daten. Dieser Modus ist standardmäßig deaktiviert.

Um die Netzwerklast zu minimieren und um Datenkollisionen zu vermeiden, sollten Sie die Hierarchiereplikation für die verschiedenen Notification Server in Ihrer Hierarchie zu unterschiedlichen Zeitpunkten einplanen.

Siehe "Konfigurieren eines Zeitplans" auf Seite 129.

Die Hierarchiereplikation synchronisiert verschiedene Typen von Objekten auf folgende Weise:

Sicherheitsobjekte	Sicherheitsobjekte, wie z. B. Rollen und Privilegien, setzen immer vollständige Replikationen ein. Differenzial-Replikation ist keine Option für schreibgeschützte Objekte dieses Typs.
Elemente	Elemente setzen Differenzial-Replikation ein; d.h., jedes Element wird mittels Hashing auf Änderungen überprüft und die Elemente, die sich geändert haben, werden repliziert.

Ressourcen	Ressourcen setzen Differenzial-Replikation ein. Differenzial-Replikation basiert auf dem Quelldaten-Zeitstempel "Zuletzt geändert". Daten, die seit der letzten Replikation geändert wurden, werden an den Zielserver repliziert. Die Daten auf dem Zielserver werden verifiziert, vorausgesetzt, dass die Datenüberprüfung in der entsprechenden Replizierungsregel aktiviert war. Die Datenüberprüfung bedeutet eine erhebliche Verarbeitungslast für den Notification Server. Zur Verringerung der Last können Sie bei jeder Replikation einen Prozentsatz der Daten auf dem Zielserver angeben. Wenn Sie z. B. 10 % der Daten bei jeder Replikation überprüfen, wird gewährleistet, dass alle Daten nach 10 Replikationen verifiziert wurden.

Diese Aufgabe ist ein Schritt beim Implementieren der Notification Server-Hierarchie.

Siehe "Implementieren der Notification Server-Hierarchie" auf Seite 163.

So konfigurieren Sie die Hierarchiereplikation und Hierarchiereplikationsregeln

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Hierarchie".
2. Klicken Sie auf der Seite "Hierarchieverwaltung" auf die Registerkarte "Replikation".
3. Konfigurieren Sie die Hierarchiereplikation, indem Sie die entsprechenden Optionen auswählen.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.
4. So konfigurieren Sie die Hierarchiereplikationsregeln

Erstellen einer neuen Hierarchiereplikationsregel	1 Klicken Sie auf "Hinzufügen". 2 Nehmen Sie im Dialogfeld "Replikationsregel" die entsprechenden Einstellungen vor. Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken. 3 Klicken Sie auf "Änderungen speichern".
Ändern einer bestehenden Replikationsregel	1 Wählen Sie die gewünschte Regel aus und klicken Sie auf "Bearbeiten". 2 Nehmen Sie im Dialogfeld "Replikationsregel" die entsprechenden Einstellungen vor. 3 Klicken Sie auf "Änderungen speichern".

Aktivieren einer Hierarchiereplikationsregel	Aktivieren Sie neben dem Namen der Replikationsregel die Option "Aktiviert".
Löschen einer Hierarchiereplikationsregel	Wählen Sie die gewünschte Regel aus und klicken Sie auf "Löschen". Die Replikationsregeln, die im Lieferumfang von Notification Server bzw. der installierten Lösungen enthalten sind, können nicht gelöscht werden. Sie können diese Regeln jedoch nach Bedarf aktivieren und deaktivieren sowie den Namen und die Beschreibung der Regeln ändern.

5 Klicken Sie auf "Änderungen speichern".

Einrichten der benutzerdefinierten Hierarchiereplikation

Sie können die benutzerdefinierte Hierarchiereplikation für Konfigurations- und Verwaltungselemente sowie Sicherheitsrollen und Privilegien einrichten.

Im Bericht der aktuellen Elementreplikation, auf den Sie im Fenster "Konfigurations- und Verwaltungselemente" zugreifen können, werden alle Elemente aufgelistet, die mithilfe der benutzerdefinierten Hierarchiereplikation für die Replikation aktiviert wurden. Wenn die ausgewählten Elemente repliziert werden, werden alle abhängigen Elemente, die nicht aktiviert wurden, automatisch eingeschlossen. Diese Elemente werden nicht im Bericht der Elementreplikation angezeigt. Um eine Liste aller Elemente anzuzeigen, die repliziert wurden, müssen Sie den Bericht "Objekte repliziert" anzeigen.

Diese Aufgabe ist ein Schritt beim Implementieren der Notification Server-Hierarchie.

Siehe "Implementieren der Notification Server-Hierarchie" auf Seite 163.

So richten Sie die benutzerdefinierte Hierarchiereplikation für Konfigurations- und Verwaltungselemente ein

1 Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Hierarchie".

2 Klicken Sie auf der Seite "Hierarchieverwaltung" auf der Registerkarte "Replikation" im Fenster "Konfigurations- und Managementelemente" auf "Benutzerdefiniert".

3 Klicken Sie auf "Änderungen speichern".

4. Klicken Sie in Symantec Management Console im linken Teilfenster mit der rechten Maustaste auf den Ordner oder das Element, den/das Sie replizieren möchten, und klicken Sie anschließend auf "Hierarchie" > "Replikation aktivieren".
5. Wenn Sie einen Ordner ausgewählt haben, geben Sie im Dialogfeld "Geerbtes Replikationsverhalten" an, ob der Ordnerinhalt in die Replikation eingefügt werden soll:

So fügen Sie den gesamten Ordnerinhalt ein	Klicken Sie auf "Ja".
So replizieren Sie nur den Ordner ohne Inhalt	Klicken Sie auf "Nein".

   Falls erforderlich, können Sie später bestimmte Unterordner manuell aktivieren oder deaktivieren.

So richten Sie benutzerdefinierte Hierarchiereplikation für Sicherheitsrollen und Privilegien ein

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Hierarchie".
2. Klicken Sie auf der Seite "Hierarchieverwaltung" auf der Registerkarte "Replikation" unter "Sicherheit" auf "Benutzerdefiniert".
3. Klicken Sie auf "Sicherheitsrollen und Privilegien auswählen".
4. Wählen Sie im Fenster "Sicherheitsrollen und Privilegien auswählen" die Rollen und Privilegien aus, die Sie replizieren möchten.
5. Klicken Sie auf "OK".
6. Klicken Sie auf "Änderungen speichern".

Übergehen des Differenzial-Replikationszeitplans für Hierarchien

Die in einer Hierarchie enthaltenen Notification Server-Computer werden normalerweise nach dem Replikationszeitplan synchronisiert, der in den Replizierungsregel eingerichtet wurde. Sie können bei Bedarf den Differenzial-Replikationszeitplan für Ihren Notification Server überschreiben und die Hierarchiereplizierungsregeln sofort auslösen. Sie löst den Differenzial-Zeitplan der Hierarchie im ausgewählten untergeordneten Knoten aus. Alle Hierarchiereplikationsregeln im Differenzial-Zeitplan werden sofort ausgeführt. Die Regeln in benutzerdefinierten Zeitplänen werden nicht ausgelöst. Sie können Daten manuell von einem übergeordneten oder untergeordneten Remote-Notification-Server an Ihren Notification Server replizieren.

Sie können die Replikation an einen Remote-Notification-Server nicht manuell überschreiben. Sie können nur Vorgänge ausführen, die sich auf Ihren Notification Server beziehen. Sie können sich bei einem Remote-Notification-Server anmelden, um diesen zu Ihrem Notification Server zu machen und dann manuell die Differenzial-Replikationszeitpläne von dessen übergeordneten oder untergeordneten Notification Servern zu übergehen.

Diese Aufgabe ist ein Schritt beim Implementieren der Notification Server-Hierarchie.

Siehe "Implementieren der Notification Server-Hierarchie" auf Seite 163.

So übergehen Sie den Differenzial-Replikationszeitplan für die Hierarchie

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Hierarchie".
2. Klicken Sie auf der Seite "Hierarchieverwaltung" auf der Registerkarte "Topologie" mit der rechten Maustaste auf den Notification Server-Computer, aus dem Daten repliziert werden sollen.
3. Klicken Sie auf "Hierarchie" > "Replizieren auf…".

   Dieser Option löst Hierarchiereplikationsregeln aus, die auf Ihren lokalen Notification Server (bei dem Sie eingeloggt sind) verweisen. Sie können keine Daten vom Remote-Notification-Server an andere Remote-Server replizieren.
4. Klicken Sie im Bestätigungsdialogfeld auf "OK".

Manuelles Replizieren ausgewählter Daten

Sie können die Replizierungsregeln für Ihren Notification Server überschreiben, indem Sie eine manuelle Hierarchiereplikation eines bestimmten Ordners oder Objekts ausführen. Bei der manuellen Replikation werden die ausgewählten Daten sofort auf den untergeordneten Notification Servern repliziert. Die Daten werden unabhängig von Replizierungszeitplänen oder davon repliziert, ob sie in den Replizierungsregeln berücksichtigt wurden.

Diese Aufgabe ist ein Schritt beim Implementieren der Notification Server-Hierarchie.

Siehe "Implementieren der Notification Server-Hierarchie" auf Seite 163.

So replizieren Sie ausgewählte Daten manuell von Ihrem Notification Server

1. Klicken Sie im linken Bereich der Symantec Management Console mit der rechten Maustaste auf den Ordner oder das Objekt, der/das repliziert werden soll.

   Wenn Sie einen Ordner auswählen, wird bei der Replikation der gesamte Inhalt (alle Unterordner-Ebenen und enthaltenen Elemente) repliziert. Alle übergeordneten Ordner (nicht aber deren Inhalt) werden ebenfalls repliziert, um die Ordnerpfade innerhalb der Struktur zu bewahren.
2. Klicken Sie auf "Hierarchie" > "Jetzt replizieren"….
3. Klicken Sie im Bestätigungsdialogfeld auf "OK".

Einrichten einer Hierarchieautomatisierungsrichtlinie

Automatisierungsrichtlinien für die Hierarchie senden E-Mail-Benachrichtigungen, wenn bestimmte Ereignisse in der Hierarchie auftreten. Sie müssen die gewünschten Richtlinien aktivieren. Beachten Sie, dass Sie die Standardrichtlinien nicht ändern können. Sie können Sie jedoch duplizieren, um neue Richtlinien zu erstellen. Sie können diese Richtlinien dann entsprechend Ihrer Anforderungen konfigurieren.

Diese Aufgabe ist ein Schritt beim Implementieren der Notification Server-Hierarchie.

Siehe "Implementieren der Notification Server-Hierarchie" auf Seite 163.

So richten Sie eine Automatisierungsrichtlinie für die Hierarchie ein

1. Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Automatisierungsrichtlinien".
2. Klicken Sie im linken Teilfenster auf eine der folgenden Richtlinien:

Kritische Hierarchiewarnmeldungen	Sendet eine E-Mail-Warnmeldung mit hoher Priorität an den Benachrichtigungssystem-Administrator, wenn eine kritische Warnmeldung auf dem lokalen Notification Server eingeht. Kritische Warnmeldungen werden auch auf der Seite "Verwaltung" auf der Registerkarte "Topologie" ausgegeben.
Hierarchie-Aktivierung/ -Deaktivierung	Sendet eine E-Mail-Warnmeldung mit hoher Priorität an den Benachrichtigungssystem-Administrator, wenn eine Hierarchiereplikation auf dem lokalen Notification Server aktiviert bzw. deaktiviert wird.
Hierarchie-Warnmeldungen	Sendet eine E-Mail-Warnmeldung mit hoher Priorität an den Benachrichtigungssystem-Administrator, wenn eine wichtige Warnmeldung auf dem lokalen Notification Server eingeht.
Änderung der Hierarchiestruktur	Sendet eine E-Mail-Warnmeldung mit hoher Priorität an den Benachrichtigungssystem-Administrator, wenn eine Notification Server der Hierarchie hinzugefügt oder daraus entfernt wird.

3. Geben Sie im rechten Teilfenster die Einstellungen der Richtlinie an und klicken Sie dann auf "Änderungen speichern".
4. Klicken Sie in der Symbolleiste auf "Einschalten".

Ausführen eines Hierarchieberichts

Sie können einen Bericht auf einem beliebigen Notification Server in der Hierarchie ausführen, um Daten aus dessen CMDB zu extrahieren. Sie sollten die Übersichtsdaten aktualisieren, bevor Sie einen Hierarchienbericht ausführen. Sie können die Übersichtsdaten je nach Bedarf aktualisieren oder Updates planen.

Siehe "Aktualisieren von Übersichtsdaten" auf Seite 178.

Einige installierte Lösungen können mit der Hierarchie verbundene Berichte bereitstellen. Diese Berichte fassen die relevanten Daten in der Hierarchie zusammen. In den Ergebnissen befindet sich eine einzelne Zeile für jeden Notification Server. Sie können den gesamten Bericht für einen bestimmten Notification Server ausführen, indem Sie auf die entsprechende Zeile doppelklicken.

Diese Aufgabe ist ein Schritt beim Implementieren der Notification Server-Hierarchie.

Siehe "Implementieren der Notification Server-Hierarchie" auf Seite 163.

So führen Sie einen Hierarchiebericht aus

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Hierarchie".
2. Klicken Sie auf der Seite "Hierarchieverwaltung" auf der Registerkarte "Topologie" mit der rechten Maustaste auf den Notification Server, für den der Bericht ausgeführt werden soll.
3. Klicken Sie auf "Berichte" und dann auf den entsprechenden Bericht.
4. Legen Sie auf der Berichtsseite die benötigten Parameter fest und aktualisieren Sie den Bericht.

   Siehe "Extrahieren von Notification Server-Berichtsergebnissen" auf Seite 462.

Aktualisieren von Übersichtsdaten

Wenn Sie Daten für Hierarchie-aktivierte Berichte erstellen müssen, können Sie die Übersichtsdaten im Task Server aktualisieren. Sie können Zusammenfassungsdaten nach Bedarf aktualisieren, ein einmaliges Update planen oder einen benutzerdefinierten Zeitplan für wiederkehrende Updates erstellen.

Ein Standard-Zeitplan führt die Aufgabe automatisch jeden Tag aus. Wenn Sie die Inventardaten täglich aktualisieren möchten, müssen Sie den Aktualisierungszeitplan dazu nicht ändern.

Diese Aufgabe ist ein Schritt im Prozess für das Implementieren der Notification Server-Hierarchie.

Siehe "Implementieren der Notification Server-Hierarchie" auf Seite 163.

So aktualisieren Sie die Übersichtsdaten bei Bedarf

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster "Notification Server > Aufgabeneinstellungen > Zusammenfassungsdaten aktualisieren".
3. Klicken Sie im Teilfenster "Zusammenfassungsdaten aktualisieren" mit der rechten Maustaste auf die Aufgabe, die Sie ausführen möchten, und klicken Sie dann auf "Jetzt starten".

   Sie können auf "Details" klicken, um weitere Informationen über die Aufgabe anzuzeigen, bevor Sie sie ausführen.
4. Erstellen Sie einen benutzerdefinierten Zeitplan, wenn der von Ihnen auszuführende Zeitplan nicht in der Liste angezeigt wird.

So erstellen Sie einen Zeitplan

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster "Notification Server > Aufgabeneinstellungen > Zusammenfassungsdaten aktualisieren".
3. Klicken Sie auf der Seite "Zusammenfassungsdaten aktualisieren" auf "Neuer Zeitplan".
4. Geben Sie im Dialogfeld "Neuer Zeitplan" die Einstellungen des Zeitplans an und klicken Sie dann auf "Zeitplan".

   Für weitere Informationen klicken Sie auf die Seite und drücken Sie dann **"F1"**.

Siehe "Ausführen eines Hierarchieberichts" auf Seite 177.

Kapitel 9

Konfigurieren der Replikation

In diesem Kapitel werden folgende Themen behandelt:

- Info zu Replikation und Replikationsregeln
- Replikationsanforderungen
- Konfigurieren von Replikationsregeln

Info zu Replikation und Replikationsregeln

Replikation ist die Datenübertragung in einer Richtung zwischen zwei Notification Servers.

Siehe "Replikationsanforderungen" auf Seite 182.

Hinweis: Replikation wird zwischen zwei Notification Servers, auf denen verschiedene Versionen von IT Management Suite installiert ist, nicht unterstützt. Beispiel: Sie können Daten nicht von einem 7.0-Server auf einen 7.1-Server replizieren.

Die hier beschriebene Standalone-Replikation unterscheidet sich von der Hierarchiereplikation. Die Standalone-Replikation definiert den Informationsfluss zwischen zwei Notification Servern. Die Hierarchiereplikation stellt zuverlässige und skalierbare Datensynchronisierung zwischen mehreren Notification Servern zur Verfügung.

Die Replikation kann so konfiguriert werden, dass Daten außerhalb der Hierarchiestruktur repliziert werden. Beispielsweise durch das Senden von Daten zu einem externen Server, der bestimmte Informationen für Berichte sammelt.

Die folgenden Replikationstypen werden unterstützt:

Differenziell	Repliziert Objekte und Daten, die seit der letzten Replikation geändert wurden. Dies ist die empfohlene Methode, weil beim Replizieren von Daten der Verbrauch der Netzwerklast und -bandbreite verringert wird.
Vollständig	Repliziert alle Objekte und Daten. Diese Methode wird häufig für die Hierarchiereplikation verwendet. Eine vollständige Replikation wird im Allgemeinen durch monatliche Durchführung sichergestellt. Die eigenständige Replikation führt im Unterschied zur Hierarchiereplikation keine vollständige Replikation aus. Die eigenständige Replikation ist immer differenzial.

Ein anderer Unterschied zwischen der Hierarchiereplikation und Replikation besteht darin, dass innerhalb einer Hierarchie die replizierten Daten gesichert und (standardmäßig) schreibgeschützt sind. Der Besitz ist zutreffend, so dass untergeordnete Notification Server die Daten, die von den übergeordneten Notification Servern abwärts repliziert wurden, nicht automatisch überschreiben können. Einige Daten enthalten die Einstellungen, wodurch er auf dem Ziel bearbeitet werden kann, und diese können entsprechend konfiguriert werden. Die Replikation hat keinen solchen Besitz, so dass alle replizierten Daten auf den Ziel-Notification Servern bearbeitet werden können.

Um die Replikation zu konfigurieren, müssen Sie auf jedem Notification Server-Computer die entsprechenden Replikationsregeln einrichten. In jeder Regel werden die Daten festgelegt, die von dem betreffenden Server (dem Quellserver) auf einem oder mehreren Zielservern repliziert werden. Außerdem wird der zu verwendende Zeitplan festgelegt.

Siehe "Konfigurieren von Replikationsregeln" auf Seite 183.

Sie können eine Replikationsregel für die folgenden Elemente erstellen:

Ereignisse	Repliziert Notification Server-Ereignisse.
Elemente	Repliziert Notification Server-Konfigurations- und Verwaltungselemente wie Richtlinien, Filter und Berichte.

Ressourcen	Repliziert Notification Server-Ressourcentypen, -Ressourcenziele und spezifische Datenklassen. Wenn Sie Ressourcenziele in eine Ressourcenreplikationsregel einschließen, müssen Sie beachten, dass die Ressourcendefinition sich nur auf den Inhalt (Ressourcen) des replizierten Ziels bezieht. Aus diesem Grund hängen die replizierten Ressourcen vom Eigentümer des Ressourcenziels ab. Der Notification Server-Administrator kann festlegen, dass Ressourcenziele in ihrem aktuellen Status (im Besitz eines anderen Benutzers mit dem entsprechenden Berechtigungsumfang) repliziert werden. Er kann sich auch die Ziele zuweisen, diese mit Administratorumfang speichern (schließt normalerweise mehr Ressourcen ein) und dann in diesem Status replizieren. Alle aktuellen Elemente eines Ressourcenziels werden repliziert. Das eigentliche Ressourcenzielelement wird im Hintergrund als abhängiges Objekt repliziert. Das Ziel, das auf eine eigenständige Regel angewendet wird, wird ebenfalls repliziert, wenn die eigenständige Regel repliziert wird. Wenn die Regel ausgeführt wird, wird das Ziel nicht gesendet.
Sicherheit	Repliziert Notification Server-Sicherheitsrollen und -rechte. Es stehen zwei Arten von Sicherheits-Replikationsregeln zur Verfügung: Recht und Rolle. Die Konfigurationsverfahren für beide sind identisch. Wenn Sie eine Sicherheitsrolle in einer Replikationsregel einschließen, müssen Sie auch eine Replikationsregel konfigurieren, um alle Rechte in der Rolle zu replizieren. Die replizierte Sicherheitsrolle erkennt keine der Privilegien an, die bereits auf dem Notification Server-Zielcomputer bestehen.

Replikationsanforderungen

Die Anforderungen für das Konfigurieren der Replikation im Benachrichtigungssystem müssen erfüllt sein, bevor Sie eine Replikation konfigurieren können.

Es gelten folgende Replikationsanforderungen:

- Netzwerkverkehr muss zwischen Notification Servern routingfähig sein
- HTTP-/HTTPS-Datenverkehr muss zwischen Notification Servern zugelassen sein
- Zwischen den Notification Servern müssen Vertrauensbeziehungen bestehen, oder es müssen Identifikationsdaten für die privilegierten Konten bekannt sein, die die Vertrauensstellung ermöglichen.

- Jeder Notification Server muss den Namen und die Netzwerkadresse der Notification Server auflösen können, mit denen er Daten repliziert.
- Es muss genug Bandbreite zwischen den Notification Server vorhanden sein, um die Paket- und Datenreplikation zu unterstützen.
  Die erforderliche Bandbreite und Hardware hängen von der Größe der Infrastruktur und der replizierten Daten ab.
- Jeder Notification Server muss über einen Site Server verfügen, der den verfügbaren Paketdienst ausführt. Der Paketdienst muss auf dem Notification Server-Computer verfügbar sein.

Siehe "Info zu Replikation und Replikationsregeln" auf Seite 180.

Konfigurieren von Replikationsregeln

Bevor Sie das Replizieren von Daten von einem Notification Server auf einen anderen beginnen, müssen Sie die Replikation planen. Damit wird sichergestellt, dass ähnliche Daten nicht in beide Richtungen weitergeleitet werden. Falls einer Ihrer Server nicht Teil einer Hierarchie ist, müssen Sie gewährleisten, dass die Replikation nicht mit dem Hierarchiereplikationsprozess in Konflikt steht. Notification Server überprüft nicht, ob Ihre Replikationskonfiguration konsistent mit der Hierarchie ist. Eine schlecht geplante Implementierung kann Datenkonflikte hervorrufen oder die betroffenen CMDBs überschreiben.

Siehe "Info zu Replikation und Replikationsregeln" auf Seite 180.

Siehe "Replikationsanforderungen" auf Seite 182.

Die Regel muss zur Ausführung für die festgelegte Replikation aktiviert werden. Sie können Replikationsregeln jederzeit dem Bedarf Ihrer Organisation entsprechend aktivieren und deaktivieren. Für jede aktivierte Regel werden die festgelegten Daten gemäß des angegebenen Zeitplans repliziert.

Sie können Daten jederzeit replizieren, indem Sie die entsprechenden Replikationsregeln ausführen. Klicken Sie in der Konsole mit der rechten Maustaste auf die Regel und wählen Sie "Ausführen". Die Ausführung einer Replikationsregel überschreitet ihren Zeitplan und repliziert die angegebenen Daten sofort an die Zielserver. Die Ausführung einer Replikationsregel ist ein einmaliger Vorgang und hat keine Auswirkung auf den Replikationszeitplan. Alle Replikationsregeln werden gemäß des Zeitplans weiterhin ausgeführt.

Hinweis: Replikation wird zwischen zwei Notification Servers, auf denen verschiedene Versionen von IT Management Suite installiert ist, nicht unterstützt. Beispiel: Sie können Daten nicht von einem 7.0-Server auf einen 7.1-Server replizieren.

So konfigurieren Sie eine Replikationsregel

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster den Ordner "Einstellungen > Notification Server > Replikation".
3. Im Ordner "Replikation" haben Sie folgende Möglichkeiten:

Eine neue Replizierungsregel erstellen	Klicken Sie mit der rechten Maustaste auf den entsprechenden Ordner und klicken Sie auf "Neu" > "Replikationsregel". Die neue Regel wird in dem Ordner angezeigt und automatisch ausgewählt.
Eine bestehende Replikationsregel ändern	Erweitern Sie den relevanten Ordner und wählen Sie dann die zu ändernde Replikationsregel aus.
Eine Replikationsregel aktivieren oder deaktivieren	Erweitern Sie den entsprechenden Ordner, klicken Sie mit der rechten Maustaste auf die Replizierungsregel und klicken Sie auf "Aktivieren" bzw. "Deaktivieren". Sie können eine Regel auch auf der Seite "Replikationsregel" aktivieren oder deaktivieren, indem Sie auf das Symbol "Regelstatus (Ein/Aus)" klicken.
Eine Replikationsregel ausführen	Erweitern Sie den entsprechenden Ordner, klicken Sie mit der rechten Maustaste auf die auszuführende Replizierungsregel und wählen Sie dann "Ausführen".

4. Legen Sie auf der Seite "Replikationsregel" die gewünschten Einstellungen fest.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.
5. Klicken Sie auf "Änderungen speichern".

Kapitel 10

Erstmalige Konfiguration

In diesem Kapitel werden folgende Themen behandelt:

- Ausüben von Konfigurationsaufgaben bei der Ersteinrichtung

Ausüben von Konfigurationsaufgaben bei der Ersteinrichtung

Beim Installieren der Symantec Management-Plattform wird Notification Server als Teil des Installationsprozesses konfiguriert. Es sind keine weiteren Konfigurationen erforderlich, um Notification Server starten zu können.

Sollten Sie dennoch die Symantec Management-Plattform ohne begleitende Versionen bestimmter Produkte installieren, werden einige Links zu den Konfigurationsseiten angezeigt. In diesem Fall müssen Sie die Plattform manuell konfigurieren.

Siehe "Info zum Konfigurieren von Notification Server" auf Seite 67.

Jedoch wenn Sie Symantec Management-Plattform und Begleitversionen von bestimmten Produkten installieren, sehen Sie eine Portalseite "Willkommen bei der Symantec Management Console", die den Erstkonfigurationsprozess vereinfacht.

Die Seite "Willkommen bei der Symantec Management Console" wird angezeigt, wenn Sie eines der folgenden Produkte installieren:

- IT Management Suite
- Server Management Suite
- Client Management Suite

Einige der in Ihrem Paket enthaltenen Lösungen müssen u. U. konfiguriert werden, damit Sie sie verwenden können. Die Portalseite "Willkommen bei der Symantec Management Console" stellt den Zugangspunkt für die Ausführung von Schlüsselkonfigurationsaktionen für Lösungen in den installierten Suites dar. Diese

Vorgänge stellen die wesentlichen Einstellungen dar, die Sie konfigurieren müssen, um mit den Lösungen arbeiten zu können.

Nach der Installationskonfiguration müssen Sie möglicherweise weitere Konfigurationsaufgaben durchführen. Die Durchführung weiterer Schritte hängt von den Produkten ab, die Sie zuerst installiert haben oder die Sie nach dem erstmaligen Setup installieren. Zusätzlich sind erweiterte Einstellungen im Menü "Einstellungen" und auch möglicherweise in anderen Bereichen von individuellen Produkten verfügbar.

Weitere Informationen zu Konfigurationsoptionen der einzelnen Lösungen und Produkte finden Sie in der Dokumentation der Produkte.

Tabelle 10-1 Prozess zur Ausübung von Konfigurationsaufgaben bei der Ersteinrichtung

Schritt	Aufgabe	Beschreibung
Schritt 1	Erkennen von Computern.	Sie müssen die Computer importieren oder erkennen, die in Ihrer Umgebung sind. Siehe "Erkennen von Computern" auf Seite 186.
Schritt 2	Führen Sie für Symantec Management-Agent und die -Lösungs-Plugins ein Rollout aus.	Nachdem Sie die Computer in Ihrer Umgebung erkennen, verteilen Sie Symantec Management-Agent und -Lösungs-Plugins auf die Computer, die Sie verwalten möchten. Siehe "Ausführen eines Rollouts für Symantec Management-Agent und -Lösungs-Plugins" auf Seite 189.
Schritt 3	Erfassen von Inventardaten.	Notification Server sammelt in diesem Schritt die Informationen, die die eben verteilten Agents auf den verwalteten Computern erfassen. Siehe "Erfassen von Inventardaten" auf Seite 193.
Schritt 4	Planen des Patch-Managements	In diesem Schritt können Sie den Download und die Installation der Software-Updates planen. Siehe "Planen des Patch-Managements" auf Seite 195.

Erkennen von Computern

Mit der Funktion "Computer entdecken" werden Computer in Ihrer Umgebung identifiziert. Bevor Sie Computer verwalten können, müssen Sie zuerst die verfügbaren Computer identifizieren und die auswählen, die Sie mit Symantec Management Agent verwalten möchten.

Um Computer zu erkennen, wählen Sie zuerst die Computertypen aus, auf denen Sie Symantec Management Agent installieren möchten. Sie erkennen Windows-Computer mit "Active Directory-Import". Sie erkennen UNIX-, Linux- und Mac-Computer mit einem Netzwerkscan (Ping Sweep) für einen von Ihnen ausgewählten IP-Adressbereich.

Diese Aufgabe ist ein Schritt im Prozess zur Ausübung von Konfigurationsaufgaben bei der Ersteinrichtung.

Siehe "Ausüben von Konfigurationsaufgaben bei der Ersteinrichtung" auf Seite 185.

So führen Sie die Computererkennung durch

1. Klicken Sie in der Symantec Management Console auf "Startseite > Notification Server Management > Ersteinrichtung".
2. Klicken Sie auf der Seite "Willkommen bei der Symantec Management Console" auf "Computer erkennen".
3. Führen Sie im Assistenten "Computer erkennen" folgende Schritte durch:

"Schritt 1-Windows"

Hiermit können Sie Windows-Computer entweder über eine Domäne oder eine Arbeitsgruppe importieren.

Hinweis: Wenn Sie Computer mit einem Netzwerkscan erkennen möchten, klicken Sie ohne eine Auswahl auf dieser Seite auf "Weiter".

So importieren Sie Windows-Computer über eine Domäne:

1. Aktivieren Sie das Kontrollkästchen, um Windows-Computer zu importieren.
2. Klicken Sie auf eine Optionsschaltfläche um auszuwählen, ob von "Microsoft Active Directory" oder über eine Domänenmitgliedschaft/WINS importiert werden soll.
3. Klicken Sie auf den Pfeil nach unten neben "Domäne oder Arbeitsgruppe", um eine Domäne oder eine Arbeitsgruppe auszuwählen. Sie können aber auch einen Domänennamen oder einen Arbeitsgruppennamen manuell eingeben.
4. Geben Sie die Domänenidentifikationsdaten ein.
5. Klicken Sie entweder auf die Option "Ein" oder "Aus" neben "Wiederkehrende Importvorgänge planen".

   Wenn Sie später neue Computer zu Ihrem Netzwerk hinzufügen möchten, lassen Sie diese Option aktiviert. Durch diese Option werden Computer automatisch erkannt, wenn Sie zu Ihrem Netzwerk hinzugefügt werden.
6. Klicken Sie auf "Zeitplan".

   Wählen Sie einen vorhandenen gemeinsam genutzten Zeitplan für den wiederkehrenden Import aus. Diese Liste wird anhand der Seite "Gemeinsam genutzte Zeitpläne" ausgefüllt. Sie können die Zeitpläne unter "Einstellungen > "Notification Server" > "Gemeinsam genutzte Zeitpläne" ändern, erstellen und gemeinsam verwenden.
7. Klicken Sie auf "Weiter".

"Schritt 2-Netzwerk"

Hiermit können Sie Computer mit einem Netzwerkscan (Ping Sweep) erkennen.

Hinweis: Wenn Sie Windows-Computer über eine Domäne oder eine Arbeitsgruppe importieren möchten, klicken Sie ohne eine Auswahl auf dieser Seite auf "Zurück"

So erkennen Sie Computer mit einem Netzwerkscan:

1. Aktivieren Sie das Kontrollkästchen, um vernetzte Computer und Geräte zu erkennen.
2. Geben Sie einen Netzwerkscanbereich ein.

   Möglicherweise müssen Sie nicht alle IP-Adressen scannen. Bei einer erstmaligen Installation müssen möglicherweise alle Subnetze einschließen um sicherzustellen, dass jedes Gerät identifiziert wird. Sie können den Bereich jedoch je nach Bedarf begrenzen. Sie können beispielsweise mehrere Scans auf bestimmten Subnetzen ausführen, wenn die Erkennungsaufgaben dadurch vereinfacht werden.
3. Wenn Sie mit Netzwerkgeräten kommunizieren und sie genauer klassifizieren möchten, klicken Sie auf "Zusätzliche Bereiche aktivieren".

   Hinweis: Wenn Sie über Remote-Zugriff keine Verbindung herstellen können, ist möglicherweise eine Firewall in Ihrem Netzwerk oder auf Ihren Computern aktiviert. Sie müssen sie deaktivieren, um die Erkennung auszuführen.
4. Wenn Sie sofort zum zweiten Installationskonfigurationsschritt übergehen möchten, aktivieren Sie "Assistent zum Symantec Agent-Rollout ausführen".

   Siehe "Ausführen eines Rollouts für Symantec Management-Agent und -Lösungs-Plugins" auf Seite 189.

4. Klicken Sie auf "Erkennen".

Ausführen eines Rollouts für Symantec Management-Agent und -Lösungs-Plugins

Mit dem Assistent "Rollout-Agent" können Sie für Symantec Management-Agent und die -Lösungs-Plugins ein Rollout an die Computer ausführen, die Sie verwalten möchten. Er optimiert auch das Rollout des Agents, basierend auf der Anzahl von Computern in Ihrer Umgebung.

Nachdem Symantec Management-Agent auf einem Clientcomputer installiert ist, sendet der Agent eine Registrierungsanfrage an Notification Server aus, eine vertrauenswürdige Kommunikation herzustellen. Basierend auf den Regeln, die Sie in den Agent-Registrierungsrichtlinien spezifizieren, ermöglicht oder blockiert Notification Server die Registrierungsanfragen automatisch. Beachten Sie, dass die Standard- Agent-Registrierungsrichtlinie alle eingehenden Anfragen akzeptiert. Wenn Sie nur angegebenen Computern ermöglichen möchten, sich automatisch auf Ihrem Notification Server zu registrieren, definieren Sie benutzerdefinierte Agent-Registrierungsrichtlinien.

Siehe "Info zu Agent-Registrierung" auf Seite 247.

Siehe "Erstellen einer Agent-Registrierungsrichtlinie" auf Seite 253.

Sie können die Registrierungsanfragen auf der Seite "Agent-Registrierungsstatus" unter "Berichte > Notification Server Management > Registrierung" prüfen und verwalten.

Siehe "Anzeigen und Verwalten des Agent-Registrierungsstatus" auf Seite 261.

Diese Aufgabe ist ein Schritt im Prozess zur Ausübung von Konfigurationsaufgaben bei der Ersteinrichtung.

Siehe "Ausüben von Konfigurationsaufgaben bei der Ersteinrichtung" auf Seite 185.

So verteilen Sie Symantec Management-Agent und die -Lösungs-Plugins

1. Klicken Sie in der Symantec Management Console auf "Startseite > Notification Server Management > Ersteinrichtung".
2. Klicken Sie auf der Seite "Willkommen bei der Symantec Management Console" auf "Rollout-Agent".

3 Wählen Sie im Assistenten "Rollout-Agent" im Bereich "Schritt 1: Computer" die Computer, auf denen Sie den Agent installieren möchten, aus und klicken Sie dann auf "Weiter".

Automatisch auf allen erkannten Computern installieren	Hiermit können Sie den Agent auf allen erkannten Computern installieren. Bei dieser Installationsoption können Sie auch einen wiederkehrenden Installationsplan von einer Dropdown-Liste auswählen. Diese Liste wird anhand der Seite "Gemeinsam genutzte Zeitpläne" ausgefüllt. Sie können die Zeitpläne unter "Einstellungen > "Notification Server" > "Gemeinsam genutzte Zeitpläne" ändern, erstellen und gemeinsam verwenden.
Nur auf ausgewählten erkannten Computern	Hier können Sie den Computernamen eingeben oder nach bestimmten Computern suchen, auf denen den Agent installiert werden soll. Diese Option zeigt eine typische Auswahlliste an. In der linken Spalte können Sie erkannten Computer suchen und auswählen. In der rechten Spalte befindet sich eine Liste mit aus der linken Spalte ausgewählten Computern. Geben Sie in der "Suchspalte" den gesamten oder nur einen Teil des Computernamens ein. Sie können auch Suchkriterien wie "XP", "Win" oder andere Buchstaben verwenden, die in einer Gruppe Ihrer bevorzugten Computernamen enthalten sind. Die "Suchspalte" listet die erkannten Computer auf, die Ihren Suchkriterien entsprechen. Verwenden Sie die Pfeiltasten, um die Computer von der "Suchspalte" in die "Auswahlspalte" zu verschieben. Beim Verschieben der Computer in die "Auswahlspalte" sehen Sie, wie sich die Anzahl der ausgewählten Computer in der Spalte unten rechts ändert. Durch diese Installationsoption können Sie Suchkriterien auch für ausgewählte erkannte Computer hinzufügen. Sie können die Ergebnisse in der ausgewählten Spalte auch verfeinern, indem Sie Computer nach Namen oder IP-Adressen suchen.

4 Wählen Sie im Bereich "Schritt 2: Plugins" die Plugins, die Sie installieren möchten, aus und klicken Sie dann auf "Weiter".

Wählen Sie die Plugins für alle installierten Lösungen aus. Wählen Sie auch die auf den Verwaltungsfunktionen basierenden Plugins aus, die Sie ausführen möchten. Beispielsweise wenn Sie Inventar erfassen möchten, stellen Sie sicher, dass die Inventar-Plugins, die für Ihre Umgebung relevant sind, eingeschaltet werden.

"Alle aktivieren"	Hiermit können Sie alle aufgelisteten Plugins aktivieren. Wenn Sie alle Plugins aktivieren, wird die linke Listenseite grün schattiert angezeigt. Wenn Sie alle Plugins deaktivieren, wird die Liste rot schattiert angezeigt.
Leiste "Ein/Aus"	Hiermit können Sie ausgewählte Plugins aktivieren bzw. deaktivieren. Eine rote Schattierung weist auf deaktivierte Plugins hin, eine grüne hingegen auf aktivierte Plugins.

5 Wählen Sie im Bereich "Schritt 3: Optimieren" die Rollout-Umgebung aus:

Produktionsumgebung	Damit können Sie das Rollout des Agents entsprechend der Anzahl von Computern in Ihrer Produktionsumgebung optimieren. Die Anzahl der Computer in Ihrer Produktionsumgebung legt die optimalen Abstände für das Herunterladen von Agent-Einstellungen und das Prüfen auf neue Aufgaben fest. Wenn Sie die Anzahl von Computern mit dem Schieberegler auswählen, passt der Assistent automatisch jene Abstände an. Siehe "Agent- und Aufgaben-Einstellungsoptionen" auf Seite 192. Klicken Sie auf "Details anzeigen" und dann auf "OK", um Einzelheiten zu der Agent- und Aufgabeneinstellung anzuzeigen.
Testumgebung (1 - 50 Computer)	Hiermit können Sie das Rollout auf nur einem Teil der installierten Computer testen.

6 Klicken Sie auf "Rollout-Agent".

Agent- und Aufgaben-Einstellungsoptionen

Im Assistent "Rollout-Agent" ist ein Schieberegler zu finden, mit dem Sie zwischen 0 und 15.000 Computer auswählen können. Basierend auf der von Ihnen ausgewählten Anzahl von Computern, optimiert der Assistent Ihr System hinsichtlich der Leistung automatisch.

Klicken Sie auf "Details anzeigen", um die optimierten Einstellungen anzuzeigen. Das Dialogfeld "Optimierte Einstellungen" zeigt an, wie oft eine neue Konfiguration für Agenteinstellungen heruntergeladen wird. Es zeigt auch die maximale Zeit zwischen Tickle-Versuchen für Aufgabeneinstellungen an.

Die Details im Assistenten werden auf die erkannten Computer, auf denen Sie den Agent installieren möchten, angewendet. Wenn Sie die Agent-Einstellungsoptionen für andere Computer einstellen oder ändern müssen, können Sie dies in der Symantec Management Console, unter "Einstellungen > Agents/Plugins > Spezifische Einstellungen" tun. Um Aufgabeneinstellungen zu optimieren, klicken Sie auf "Einstellungen > Notification Server > Site Server-Einstellungen", und dann im linken Teilfenster auf "Standortverwaltung > Einstellungen > Task Service > Task Service-Einstellungen". Im rechten Teilfenster stellen Sie "Minimalzeitraum zwischen Tickle-Versuchen" ein.

Siehe "Ausführen eines Rollouts für Symantec Management-Agent und -Lösungs-Plugins" auf Seite 189.

Tabelle 10-2 Optionen für die optimalen Agent- und Aufgabeneinstellungen

Anzahl der Computer in der Produktionsumgebung	Optimierte Agent-Einstellungen	Optimierte Aufgabeneinstellungen
0 - 100	5 Minuten	1 Minute
100 - 5000	eine Stunde	5 Minuten
5000 - 10000	zwei Stunden	5 Minuten
10000 - 15000	drei Stunden	5 Minuten
15000 +	vier Stunden	5 Minuten

Erfassen von Inventardaten

Das Erfassen erster Inventarisierungsinformationen ist der Schlüssel zur Verwaltung Ihres Netzwerks. Alle Lösungen verwenden Inventardaten, und die im Inventar enthaltenen Informationen werden in den Computeransichten, Softwareansichten und anderen Seiten und Feldern in der Konsole wiedergegeben. Die Kenntnis über die in Ihrem Netzwerk installierte Software ist überaus wichtig, um die Erfassung der richtigen Daten vorzunehmen, damit grundlegende Entscheidungen getroffen werden können.

Ihr Netzwerk ist eindeutig. Legen Sie daher fest, welche Informationen, bzw. über welche Ressource Sie Informationen erfassen möchten und wie oft diese Informationen erfasst werden sollen.

Sie können im Richtlinienfenster "Inventar erfassen" die Richtlinie deaktivieren oder aktivieren. Wählen Sie auch einen Standardzeitplan oder benutzerdefinierten Zeitplan aus, um sicherzustellen, dass die Richtlinie aktuell ist. Überlegen Sie sich, bevor Sie die Inventarisierungsinformationen erfassen, welche Informationen Sie im Auge behalten müssen und wie oft Sie diese Informationen aktualisieren möchten. Sie sollten auch an die eventuell vorhandenen Umstände einer Deaktivierung der Inventarisierungsrichtlinie bedenken. Die Richtlinie ist standardmäßig aktiviert.

Sie können die folgenden Arten von Inventardaten erfassen:

Hardware und Betriebssystem	Hiermit können Sie Inventardaten von CPUs, Festplatten, Arbeitsspeicher, Firmware, Benutzern und Gruppen erfassen.
Software	Hiermit können Sie Inventardaten von Windows-Programmen und "UNIX/Linux/Mac"-Softwarepaketen erfassen.
Dateieigenschaften	Hiermit können Sie Informationen über Hersteller, Versionen, Dateigrößen und interne Namen erfassen.
Serveranwendungen	Mit Inventory Pack für Server können Sie Informationen über Serveranwendungen erfassen, sofern installiert.

Diese Aufgabe ist ein Schritt im Prozess zur Ausübung von Konfigurationsaufgaben bei der Ersteinrichtung.

Siehe "Ausüben von Konfigurationsaufgaben bei der Ersteinrichtung" auf Seite 185.

So erfassen Sie Inventardaten

1. Klicken Sie in der Symantec Management Console auf "Startseite > Notification Server Management > Ersteinrichtung".
2. Klicken Sie auf der Seite "Willkommen bei der Symantec Management Console" auf "Inventar erfassen".
3. Lassen Sie die Richtlinie im Richtlinienfenster "Vollständiges Inventar erfassen" neben "Richtlinienregeln/-aktionen" aktiviert.

   Wenn Sie Richtlinie für eine gewisse Zeit nicht ausführen möchten, klicken Sie auf "Aus", um die Richtlinie zu deaktivieren.
4. Wählen Sie einen Zeitplan für die ständige Aktualisierung der Richtlinie aus. Sie können einen Standardzeitplan auswählen oder einen benutzerdefinierten Zeitplan erstellen.

   Diese Zeitplanliste wird anhand der Seite "Gemeinsam genutzte Zeitpläne" ausgefüllt. Sie können die Zeitpläne unter "Einstellungen > "Notification Server" > "Gemeinsam genutzte Zeitpläne" ändern, erstellen und gemeinsam verwenden.

5 Überprüfen Sie im Richtlinienfenster "Vollständiges Inventar erfassen" die Inventarisierungsdetails und wählen Sie die Typen des Inventars aus, die Sie erfassen möchten. Nehmen Sie gegebenenfalls Änderungen vor.

   Klicken Sie im Bereich "Richtlinienregeln/-aktionen" auf "Erweitert", um weitere Informationen über die von Ihnen ausgewählten Inventarisierungstypen zu erhalten. Sie können zusätzliche Elemente auswählen, die Sie erfassen möchten. Wenn Sie Änderungen vornehmen, klicken Sie auf "OK".

6 Überprüfen Sie die Details im Richtlinienfenster "Vollständiges Inventar erfassen" im Bereich "Gilt für/Compliance".

   Dieser Bereich zeigt weitere Informationen über das Inventar an, das auf Zielcomputern erfasst wird. Sie können die Richtlinieneinhaltung hinsichtlich der Inventarisierungsrichtlinie überprüfen, Inventardaten erfassende Computer ändern und andere Änderungen falls erforderlich vornehmen.

7 Klicken Sie auf "Änderungen speichern".

Planen des Patch-Managements

Mithilfe des Assistenten Patch planen können Sie festlegen, wann Softwareupdatedefinitionen heruntergeladen werden sollen, wie oft die Computer nach verfügbaren Updates durchsucht werden soll und wann die Updates installiert werden sollen. Sie können auch die Benachrichtigungen festlegen, die Sie erhalten möchten.

Diese Aufgabe ist ein Schritt bei der Durchführung der Konfigurationsaufgaben zur Ersteinrichtung.

Siehe "Ausüben von Konfigurationsaufgaben bei der Ersteinrichtung" auf Seite 185.

So planen Sie das Patch-Management

1 Klicken Sie in der Symantec Management Console auf "Startseite > Notification Server Management > Ersteinrichtung".

2 Klicken Sie auf der Seite "Willkommen bei Symantec Management Console" auf "Patch planen".

3 Führen Sie im Assistenten "Patch planen" die folgenden Schritte durch:

Schritt 1: Herunterladen	Hiermit können Sie den Zeitplan für das Herunterladen der Softwareupdatedefinitionen angeben. Hinweis: Wenn Sie das Herunterladen der Softwareupdatedefinitionen für ein Betriebssystem aktivieren, werden alle Anbieter unter diesem Betriebssystem automatisch für das Herunterladen ausgewählt.
Schritt 2: Benachrichtigungen	Hiermit können Sie die Benachrichtigungen festlegen, die Sie erhalten möchten.
Schritt 3: Scannen und Updates installieren	Hiermit können Sie festlegen, wie oft die Computer nach verfügbaren Updates durchsucht werden sollen und wann die Updates installiert werden sollen.

4 Klicken Sie auf "Patch planen".

Abschnitt 3

Erkennen der Ressourcen im Netzwerk

- Kapitel 11. Erkennen von Windows-Computern
- Kapitel 12. Importieren von Ressourcen aus Active Directory
- Kapitel 13. Erkennen von Netzwerkgeräten

Kapitel 11

Erkennen von Windows-Computern

In diesem Kapitel werden folgende Themen behandelt:

- Ressourcenerkennungsmethoden
- Erkennungsmethoden für Windows-Computer
- Erkennen von Computern mit der Domänen-Ressourcenerkennung

Ressourcenerkennungsmethoden

Die Erkennung aller Ressourcen in Ihrem Netzwerk ist einer der ersten Schritte auf dem Weg zur erfolgreichen Netzwerkverwaltung. Die Symantec Management-Plattform umfasst Tools zur automatischen Erkennung von Geräten in Ihrem Netzwerk. Außerdem erstellt sie Ressourcen für die in der Configuration Management Database (CMDB) erkannten Geräte. Durch die automatische Ressourcenerkennung entfällt die zeitraubende und fehleranfällige manuelle Eingabe.

Sie können jederzeit einen manuellen Erkennungsvorgang ausführen oder einen Zeitplan dafür erstellen. Durch geplante Erkennungsvorgänge können Sie die CMDB-Ressourcen für neue Computer automatisch erstellen, sobald diese dem Netzwerk hinzugefügt werden.

Tabelle 11-1 Ressourcenerkennungsmethoden

Methode	Beschreibung
Domänenressourcenerkennung	Wenn Sie Windows-Computer schnell erkennen möchten, verwenden Sie die Domänenressourcenerkennung. Diese Methode macht Computer ausfindig, die über ein Vertrauenskonto in einer Domäne verfügen. Bei der Installation von Notification Server haben Sie die Möglichkeit, Computer anhand dieser Methode automatisch zu erkennen. Siehe "Erkennungsmethoden für Windows-Computer" auf Seite 199.
Active Directory-Import	Außerdem können einige oder alle Ressourcen von Ihrem Microsoft Active Directory in die CMDB importiert werden. Sie können Ressourcenimportregeln konfigurieren, um die gewünschten Ressourcen zu identifizieren und zu importieren. Sie können dann Zeitpläne konfigurieren, um volle Importe durchzuführen und Importe in den gewünschten Abständen zu aktualisieren. Siehe "Erkennungsmethoden für Windows-Computer" auf Seite 199.
Network Discovery	Wenn Sie alle Ressourcen auf allen Plattformen erkennen möchten, verwenden Sie Network Discovery. Mit Network Discovery können Sie alle an Ihr Netzwerk angeschlossenen IP-Geräte erkennen: Router, Switches, Hubs, Netzwerkdrucker, Novell NetWare-Server sowie Windows-, UNIX- und Macintosh-Computer. Siehe "Info zu Network Discovery" auf Seite 216.

Erkennungsmethoden für Windows-Computer

Bevor Sie Computer verwalten können, müssen Sie folgende Schritte ausführen:

- Erkennen der Computer im Netzwerk
- Erstellen von Ressourcen für die Computer in der CMDB.

Sie können die Computer erkennen, auf denen Symantec Management-Agent und verschiedene Lösungs-Agenten/-Plugins installieren können.

Sie können Windows-Computer folgendermaßen erkennen:

- Suche nach allen Windows-Computern in Ihrem Netzwerk, die in einer bestimmten Domäne registriert sind
- Suche nach allen Windows-Computern in Ihrem Netzwerk, die mit den von Ihnen angegebenen Organisationseinheiten übereinstimmen

Zur Erkennung von Computern mit anderen Betriebssystemen können Sie Network Discovery verwenden.

Siehe "Ressourcenerkennungsmethoden" auf Seite 198.

Tabelle 11-2 Erkennungsmethoden für Windows-Computer

Methode	Beschreibung
Ressourcenerkennung	Durchsucht die angegebene Domäne nach allen Computern, die in dieser Domäne registriert sind. Sie müssen eine mindestens eine der Optionen "Domänensuchliste" oder "Domänenmitgliedschaft" auswählen. Siehe "Erkennen von Computern mit der Domänen-Ressourcenerkennung" auf Seite 200.
Microsoft Active Directory Import	Lässt Sie die Computerressourcen importieren, die den angegebenen Organisationseinheiten entsprechen. Sie können Computer filtern, die innerhalb einer bestimmten Anzahl von Tagen aktiv gewesen sind, oder die ein bestimmtes Windows-Betriebssystem ausführen. Diese Methode gibt ausführliche Information zu den Betriebssystemen für jeden Ihrer erkannten Computer zurück und ist die bevorzugte Methode. Siehe "Importieren von Ressourcen mit Microsoft Active Directory-Import" auf Seite 207.

Mit diesen Erkennungsmethoden können Sie alle Ihre Computer in Domänen erkennen oder die Computer in einer einzigen Domäne.

Erkennen von Computern mit der Domänen-Ressourcenerkennung

Sie können Windows-Computer durch Suchen nach Domänen-Ressourceninformationen erkennen. Für erkannte Computer wird eine Ressource in der CMDB erstellt. Sie können die Erkennung manuell oder anhand eines Plans ausführen. Nach dem Ausführen der Erkennungs können Sie die Berichte mit den Ergebnissen anzeigen.

Diese Datenbank enthält folgende Informationen für jeden erkannten Computer:

- Name (Domänensuchliste und Domänenmitgliedschaft)
- Betriebssystemname (Domänensuchliste und Domänenmitgliedschaft)
- Hauptversion (Domänensuchliste)
- Nebenversion (Domänensuchliste)
- Plattform (Domänensuchliste)

Siehe "Erkennungsmethoden für Windows-Computer" auf Seite 199.

Hinweis: Die Statusmeldung auf der Seite "Ressourcenerkennung" zeigt an, wann die Erkennung zum letzten Mal manuell von der Seite aus durchgeführt wurde. Die Zeit wird nicht aktualisiert, auch wenn später geplante Erkennungen ausgeführt wurden.

So erkennen Sie Computer mit der Domänen-Ressourcenerkennung

1. Klicken Sie in der Symantec Management Console im Menü "Aktionen" auf "Erkennen > Domänenmitgliedschaft/WINS importieren".
2. Geben Sie auf der Seite "Domänenmitgliedschaft/WINS-Import" unter "Zu durchsuchende Domänen" den Namen einer Domäne ein, die Sie durchsuchen möchten und klicken Sie dann auf das Symbol "Hinzufügen".
3. (Optional) Um einen anderen Benutzernamen und Kennwort für die Domäne einzugeben, damit der Notification Server Zugriff hat, führen Sie folgende Schritte aus:
   - Wählen Sie die Domäne aus.
   - Klicken Sie auf das Bleistiftsymbol.
   - Klicken Sie auf "Diese Identifikationsdaten verwenden".
   - Geben Sie den Benutzernamen und das Kennwort ein und klicken Sie dann auf "OK".
4. Wählen Sie mindestens eine der folgenden Optionen aus:

Domänensuchliste

Diese Methode ist für kleine, Peer-to-Peer-Umgebungen gedacht.

Die Methode nutzt die Netzwerksuchliste, um alle Computer in der Domäne zu erkennen. Die Suchoption erkennt alle Computer, die Dateien oder Drucker gemeinsam nutzen oder den Windows Messenger-Dienst ausführen (z. B. Computer mit Windows NT/2000/Server 2003/Server 2008/95/98/98 SE/ME/XP/7/8).

Diese Methode kann auch Computer in einer Arbeitsgruppe erkennen, die die Suchkriterien erfüllen.

Die Domänensuchliste zählt die Datensätze in der Computersuchliste auf. Diese Computersuchliste ist für eine kleine Peer-to-Peer-Umgebung vorgesehen und passt sich daher nicht gut an umfangreiche Umgebungen an.

Wenn der Notification Server eine Domänen-Suchlistenerkennung durchführt, fordert er die Computersuchliste an. Diese Suchliste enthält zusätzliche Informationen wie z. B. Betriebssystem und Betriebssystemversion des Computers. Dann macht er die IP-Adresse des Computers mithilfe eines Reverse-Lookups ausfindig.

In folgenden Fällen können Probleme bei der Computererkennung mit dieser Methode auftreten:

- Wenn sich der Computer nicht auf der Computersuchliste befindet.
- Wenn sich der Computer auf der Computersuchliste befindet, jedoch nicht für die gemeinsame Dateinutzung registriert ist.
- Es kann 15 bis 51 Minuten dauern, bis die Änderungen in die Computersuchliste eingetragen werden.

Die Erkennungsmethode "Domänen-Suchlistenerkennung" nimmt so viel von der Computersuchliste auf wie möglich, und das so schnell wie möglich. Diese Methode kann einen PDC in einer großen Domäne oder einer Umgebung mit mehreren Domänen überlasten. Symantec empfiehlt, diesen Vorgang außerhalb der Geschäftszeiten ausführen, vorzugsweise an einem Wochenende.

Domänenmitgliedschaft

Diese Option erkennt alle Computer in der Domäne mit Vertrauenskonten. Sie kann Computer in Windows NT 4.0-Domänen oder Windows 2000 und neueren Active Directory-Domänen erkennen. Diese Methode sucht alle Computer mit Windows NT/2000/Server 2003/Server 2008/XP/7/8 in der Domäne. Computer mit Windows 95/98/98 SE/ME werden nicht erkannt.

Hinweis: Für Computer in NT 4.0-Domänen können nur begrenzte Informationen erkannt werden. So ist zum Beispiel das spezifische Betriebssystem des Computers nicht bekannt.

Die Domänenmitgliedschaftserkennung zählt die Computerkonten in den angegebenen Domänen auf.

Wenn Sie einen Computer mit Windows NT/2000/Server 2003/Server 2008/XP/7/8 einer Domäne hinzufügen, wird in dieser Domäne ein Computerkonto erstellt. Der Computer verwendet dieses Konto zur Authentifizierung der Domäne, sodass der Computer Benutzer-Logins über eine sichere Verbindung authentifizieren kann. Für Windows 9x-Computer wird kein Computerkonto erstellt. Daher können Sie Windows 9x-Computer mit dieser Methode nicht finden.

Wenn Computer mithilfe der Domänenmitgliedschafts-Methode erkannt werden, katalogisiert Notification Server diese Konten. Anders als bei der Domänensuchlisten-Methode enthalten diese Konten keine zusätzlichen Informationen, sondern nur den Computernamen. Notification Server macht auch hier die IP-Adresse des Computers mithilfe eines Reverse-Lookups ausfindig.

5 Wählen Sie eine der folgenden Optionen aus:

Jetzt erkennen	Klicken Sie auf "Jetzt erkennen".
Zeitplan einstellen	Geben Sie unter "Zeitplanoptionen" in der Dropdown-Liste "Zeitplan" den Zeitplan für den Import an.

6 Klicken Sie auf "Änderungen speichern".

7 So zeigen Sie die Erkennungsergebnisse an

- Klicken Sie auf "Erkennungsberichte ansehen".

- Klicken Sie im Fenster "Ressourcenerkennungsberichte" mit der rechten Maustaste auf einen Bericht und klicken Sie dann auf "In neuem Fenster öffnen".
- Geben Sie die Parameter für den Bericht ein.
- Klicken Sie auf "Aktualisieren".

Kapitel 12

Importieren von Ressourcen aus Active Directory

In diesem Kapitel werden folgende Themen behandelt:

- Info zu Microsoft Active Directory-Import
- Importieren von Ressourcenzuordnungen
- Importieren von Ressourcen mit Microsoft Active Directory-Import

Info zu Microsoft Active Directory-Import

Mit der Funktion "Microsoft Active Directory-Import" von Symantec Management-Plattform können Sie Active Directory-Objekte, beispielsweise Benutzer, Computer, Sites und Subnetze, in CMDB importieren. Mit dieser Funktion können Sie die Daten nutzen, die bereits im Active Directory vorhanden sind, ohne sie neu zu erstellen. Sie können regelmäßige Importe planen, um CMDB mit aktuellen Ressourcen gefüllt zu lassen, wodurch eine bessere Verwaltung Ihrer Umgebung möglich ist.

Microsoft Active Directory-Import verwendet Lightweight Directory Access Protocol (LDAP), um eine Einwegsynchronisierung vom Active Directory zu Symantec Management-Plattform zu ermöglichen. LDAP ist dasselbe Protokoll, das von Active Directory-Standardadministrationstools verwendet wird. Microsoft Active Directory-Import unterstützt Windows 2000/2003/2008-Domänen.

Um Microsoft Active Directory-Import zu verwenden, müssen Sie die passenden Ressourcenimportregeln definieren, um die gewünschten Ressourcen zu importieren. Sie können die Ressourcenimportregeln in regelmäßigen Abständen planen und sie jederzeit manuell ausführen. Wenn Sie eine Ressourcenimportregel ausführen, können Sie alle passenden Daten (vollständiger Import) importieren. Ansonsten können Sie die Daten importieren, die neu sind oder im Active Directory seit dem

vorherigen Import (Update-Import) geändert wurden. Als Teil des Importprozesses können Sie Filter oder Organisationsgruppen automatisch auf Basis der Organisationseinheiten sowie Sicherheits- und Verteilungsgruppen erstellen, die im Active Directory eingerichtet sind. Diese Filter können verwendet werden, um Ressourcenziele anzugeben, auf die Richtlinien und Aufgaben angewendet werden.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Siehe "Importieren von Ressourcen mit Microsoft Active Directory-Import" auf Seite 207.

Während des Importprozesses werden die Computer vom Active Directory mit den verwalteten Computern in CMDB unter Verwendung des Computernamens und der Domäne abgeglichen. Jedoch importiert Microsoft Active Directory-Import alle Computer, die die Ressourcenimportregeln identifizieren, unabhängig von ihrem Symantec Management-Agent-Installationsstatus. Durch Importieren aller Computer können Sie die neuen und nicht verwalteten Computer importieren und anschließend jene Computer als Ziel für die Symantec Management-Agent-Installation angeben.

Hinweis: Sie können auch neue und nicht verwaltete Windows-Computer mithilfe der Ressourcenerkennung erkennen.

Siehe "Erkennungsmethoden für Windows-Computer" auf Seite 199.

Wenn Fehler beim Importprozess auftreten, können Sie das Statusprotokoll von Symantec Management-Plattform auf Informationen prüfen. Das Statusprotokoll können Sie über das Startmenü auf dem Symantec Management-Plattform-Computer aufrufen: "Alle Programme" > "Symantec" > "Diagnose" > "Altiris Log Viewer".

Symantec Management-Plattform enthält einige Berichte, die Informationen über Microsoft Active Directory-Importaktivitäten bereitstellen. Diese Berichte werden im Ordner "Berichte" > "Notification Server-Verwaltung" > "Microsoft Active Directory" gespeichert.

Importieren von Ressourcenzuordnungen

Microsoft Active Directory speichert nicht nur Objekte, sondern auch Beziehungen zwischen Objekten. Microsoft Active Directory-Import kann diese Beziehungen aus Active Directory extrahieren und die passenden Ressourcen sowie Ressourcenzuordnungen in CMDB erstellen. Microsoft Active Directory-Import unterstützt vier Ressourcenzuordnungen für Benutzer und eine Ressourcenzuordnung zwischen Subnetzen und Sites.

Tabelle 12-1 Von Microsoft Active Directory-Import unterstützte Ressourcenzuordnungen

Ressourcenzuordnung	Beschreibung
Benutzer - Unternehmen	Erstellt eine Unternehmensressource für den importierten Benutzer, basierend auf seinem Attribut "Unternehmen" im Active Directory.
Benutzer - Abteilung	Erstellt eine Abteilungsressource für den importierten Benutzer, basierend auf seinem Attribut "Abteilung" im Active Directory.
Benutzer - Benutzer	Erstellt eine oder mehrere Benutzerressourcen für den importierten Benutzer, basierend auf seinem Attribut "directReports" im Active Directory.
Benutzer - Benutzer	Erstellt eine Benutzerressource für den importierten Benutzer, basierend auf seinem Attribut "Manager" im Active Directory.
Site - Subnetz	Erstellt eine oder mehrere Subnetzressourcen für die importierte Site, basierend auf ihrem Attribut "siteObjectBL" im Active Directory.
Subnetz - Site	Erstellt eine Site-Ressource für das importierte Subnetz, basierend auf seinem Attribut "siteObject" im Active Directory.

Im Fenster "Ressourcenzuordnungen aktivieren" können Sie diese Beziehungen in einer Ressourcenimportregel verwenden, um andere zugehörige Ressourcen zu importieren, die nicht ausdrücklich in der Regel angegeben sind. Standardmäßig sind alle verfügbaren Ressourcenzuordnungen aktiviert.

Siehe "Erstellen und Ändern von Ressourcenimportregeln" auf Seite 209.

Importieren von Ressourcen mit Microsoft Active Directory-Import

Sie können alle Computer importieren, die in Ihrem Active Directory registriert sind. Sie können auch wählen, nur die Computer zu importieren, die den angegebenen Kriterien entsprechen.

Siehe "Info zu Microsoft Active Directory-Import" auf Seite 205.

Wenn Sie die Symantec Management-Plattform installieren, können Sie Microsoft Active Directory-Import verwenden, um alle Ihre Computer zu importieren. Danach können Sie die Installation von Symantec Management-Agent auf den nicht verwalteten Computern ausführen. Microsoft Active Directory-Import ist die

bevorzugte Methode zur Identifikation der neuen und nicht verwalteten Computer. Sie gibt ausführliche Information über die Betriebssysteme auf jedem der erkannten Computer zurück.

Sie können "Microsoft Active Directory-Import" auch verwenden, um Symantec Management-Plattform-Konten und -Rollen von Windows-Benutzern und -Gruppen zu erstellen. Sie importieren Windows-Benutzer und -Gruppen, damit Sie die Symantec Management-Plattform-Konten und -Rollen nicht manuell erstellen müssen. Microsoft Active Directory-Import besitzt eine Ressourcenimportregel für das Importieren von Rollen- und Kontoressourcen. Wenn diese Regel ausgeführt wird, kopiert sie den Windows-Benutzer und die Gruppenstruktur auf die Symantec Management-Plattform. Es wird ein Symantec Management-Plattform-Konto für alle Windows-Benutzer der ausgewählten Sicherheitsgruppen erstellt. Zusätzlich werden Symantec Management-Plattform-Rollen für jede der ausgewählten Sicherheitsgruppen erstellt. Die neu erstellten Symantec-Betriebskonten werden schließlich mit den Symantec Management-Plattform-Rollen zusammengeführt, in denen der entsprechende Windows-Benutzer in die entsprechende Windows-Gruppe eingefügt ist.

Nach dem Import können Sie Ressourcenimportregeln konfigurieren, die Active Directory regelmäßig auf neue oder geänderte Ressourcen prüfen und die erforderlichen Ressourcen in die CMDB importieren.

Wenn Sie Ressourcenimportregeln konfigurieren, können Sie die Active Directory-Quellstruktur angeben, aus der importiert werden soll. Sie können Beschränkungen anwenden, die die importierten Computer entsprechend Ihrer Anforderungen filtern. Beispielsweise können Sie nur die Computer importieren, die innerhalb einer bestimmten Anzahl von Tagen das Kennwort des Benutzerkontos geändert haben oder die Computer, die ein bestimmtes Windows-Betriebssystem ausführen.

Tabelle 12-2 Prozess zum Import der Ressourcen mit Hilfe von Microsoft Active Directory-Import

Schritt	Aktion	Beschreibung
Schritt 1	Konfigurieren der erforderlichen Ressourcenimportregeln.	Sie können neue Ressourcenimportregeln erstellen oder die vorhandenen Regeln ändern, um Ihren Anforderungen zu entsprechen. Sie können auch Regeln löschen, die Sie nicht mehr benötigen. Siehe "Erstellen und Ändern von Ressourcenimportregeln" auf Seite 209.
Schritt 2	Planen Sie die Ressourcenimportregeln.	Für jede Ressourcenimportregel können Sie volle Importe planen und Importe in gewünschten Abständen aktualisieren. Siehe "Planen von Ressourcenimportregeln" auf Seite 212.

Schritt	Aktion	Beschreibung
Schritt 3	Konfigurieren des Directory-Synchronisierungszeitplans.	Der Zeitplan für die Verzeichnissynchronisierung identifiziert zuvor importierte Ressourcen, die nicht mehr im Active Directory existieren und entfernt sie aus der CMDB. Siehe "Konfigurieren des Zeitplans für Verzeichnissynchronisierung" auf Seite 213.
Schritt 4	(Optional) Manuelles Ausführen einer Ressourcenimportregel.	Sie können eine Ressourcenimportregel jederzeit manuell ausführen. Sie können die Regel als vollen Import oder ein Importupdate ausführen. Siehe "Manuelles Ausführen von Ressourcenimportregeln" auf Seite 214.

Erstellen und Ändern von Ressourcenimportregeln

Mithilfe von Ressourcenimportregeln können Sie die Ressourcen angeben, die Sie aus Active Directory importieren möchten.

Sechs Standardressourcenimportregeln werden mit der Symantec Management-Plattform bereitgestellt, eine für jeden der unterstützten Ressourcentypen: "Benutzer", "Computer", "Druckerwarteschlage", "Site", "Subnetz" und "Rolle und Account". Sie können diese Regeln Ihren Anforderungen entsprechend ändern, oder Sie können neue Regeln erstellen, um die gewünschten Ressourcen zu importieren.

Sie können eine Regel konfigurieren, um Filter oder Organisationsgruppen automatisch auf Basis der Active Directory-Organisationseinheiten, -Sicherheitsgruppen und -Verteilungsgruppen zu erstellen, über die die Regel Ressourcen importiert. Diese Filter können anschließend verwendet werden, um Ressourcenziele anzugeben, auf die Richtlinien und Aufgaben angewendet werden.

Sie können Ihre Ressourcenimportregeln planen, um CMDB in regelmäßigen Abständen zu aktualisieren, oder Sie können eine bestimmte Regel jederzeit manuell ausführen. Durch Ausführen Ihrer Ressourcenimportregeln von Zeit zu Zeit wird sichergestellt, dass sich Änderungen am Active Directory in CMDB wiederspiegeln.

Diese Aufgabe ist ein Schritt beim Importieren von Ressourcen mit Microsoft Active Directory-Import.

Siehe "Importieren von Ressourcen mit Microsoft Active Directory-Import" auf Seite 207.

So erstellen oder ändern Sie eine Ressourcenimportregel

1. Klicken Sie in Symantec Management Console im Menü "Aktionen" auf "Erkennen" > "Microsoft Active Directory importieren".
2. Führen Sie auf der Seite "Microsoft Active Directory-Import" eine der folgenden Aufgaben durch:

So erstellen Sie eine neue Ressourcenimportregel	Klicken Sie in der Symbolleiste auf das Symbol "Neue wichtige Regel erstellen". Die neue Regel wird zur Liste der Ressourcenimportregeln hinzugefügt.
So ändern Sie eine vorhandene Ressourcenimportregel	Wählen Sie in der Liste der Ressourcenimportregeln die passende Regel aus.
So löschen Sie eine Ressourcenimportregel	Wählen Sie in der Liste von Ressourcenimportregeln, die entsprechende Regel und klicken Sie dann in der Symbolleiste auf "Ausgewählte Importregel löschen".

3. Klicken Sie in der Ressourcenimportregel, die Sie ändern möchten, für jeden der hervorgehobenen Links auf den Link, und geben Sie anschließend die passenden Einstellungen an.

"Angegebener Ressourcentyp" (Standardeinstellung), Computer, Benutzer, Site, Subnetz	Geben Sie den Domänen- und Ressourcentyp, den Sie importieren möchten, und die passende Active Directory-Quellstruktur an.
Angegebene Datenquelle (Standardeinstellung)	Geben Sie die Domäne oder den Server (Domänencontroller) und die passenden Kontoidentifikationsdaten an, über die/mit denen Sie Ressourcen importieren möchten.

Keine (Standardeinstellung)	Wenn Sie auf diesen Link klicken, wird eines der folgenden Dialogfelder angezeigt: ■ Organisationseinheit (OE) auswählen Wählen Sie die Active Directory-Organisationseinheiten oder -Container (welche auch immer der im Fenster "Ressourcenauswahl" angegebenen Quellstruktur entsprechen) aus, über die Ressourcen importiert werden sollen. Wenn Sie eine Organisationseinheit oder einen Container auswählen, können Sie wählen, ob ihre/seine untergeordneten Elemente enthalten sein sollen. ■ "Sicherheitsgruppen auswählen" oder "Verteilungsgruppen auswählen" Wählen Sie die bestimmten Active Directory-Gruppen aus, aus denen Benutzer und Gruppen importiert werden sollen. Das Dialogfeld "Sicherheitsgruppen auswählen" wird nur für die Regel angezeigt, die Rollen- und Kontoressourcen importiert.
"Angegebene Spaltenzuordnungen" (Standardeinstellung), Standardspalten-zuordnungen	Geben Sie die Zuordnung zwischen den Symantec Management-Plattform-CMDB- und Active Directory-Ressourcendatenfeldern an. Sie können mithilfe dieser Zuordnungen zusätzliche Attribute importieren, wenn das Active Directory-Schema erweitert wurde.
"Alle Computer", "Alle Benutzer"	Geben Sie die passenden Kriterien an, um die importierten Ressourcen nur auf diejenigen zu beschränken, die den angegebenen Kriterien entsprechen. Eine Ressource wird nur importiert, wenn sie alle angegebenen Kriterien erfüllt.
Diese Ressourcen-zuordnungen	Geben Sie die Ressourcenzuordnungen an, die Sie zum Importieren anderer zugehöriger Ressourcen verwenden möchten, die nicht ausdrücklich in der Ressourcenimportregel angegeben werden. Standardmäßig sind alle verfügbaren Ressourcenzuordnungen aktiviert. Microsoft Active Directory-Import kann diese Beziehungen aus Active Directory extrahieren und die passenden Ressourcen sowie Ressourcenzuordnungen in CMDB erstellen. Siehe "Importieren von Ressourcenzuordnungen" auf Seite 206.
Angegebene Zeitpläne	Legen Sie die Zeitpläne zum Importieren von Ressourcen fest. Sie können Zeitpläne für vollständige und Update-Datenimporte festlegen. Siehe "Planen von Ressourcenimportregeln" auf Seite 212.

4 Aktivieren Sie die entsprechenden Kontrollkästchen "Aktiviert", um das Importieren von Computer-, Benutzer-, Subnetz- und Site-Ressourcen zu aktivieren.

5 Klicken Sie auf "Übernehmen".

Planen von Ressourcenimportregeln

Sie können für jede Ressourcenimportregel die erforderlichen Zeitpläne für vollen Import und Import-Updates angeben. Ein voller Import importiert alle Ressourcen vom Ziel-Domänencontroller oder der Domäne. Ein Import-Update importiert nur die Ressourcen, die seit der letzten Import geändert wurden.

Eine einzelne Ressourcenimportregel kann beide Zeitpläne umfassen oder Sie können verschiedene Regeln für den vollen Import und Import-Updates konfigurieren. Wenn Sie eine Import-Update-Regel konfigurieren, empfehlen wir, dass die Regel auf einen Domänencontroller anstatt eine Domäne abzielt.

Ein Import-Update wird als voller Import ausgeführt, wenn eine der folgenden Aussagen zutrifft:

- Die Regel wird zum ersten Mal ausgeführt.
- Die Domäne oder der Server, die in der Regel angegeben ist, wurde geändert.
- Der Domänencontroller, den die Regel zuvor importiert hat, ist nicht verfügbar ist.

Bei Bedarf können Sie den Zeitplan aufheben und eine Ressourcenimportregel jederzeit manuell ausführen.

Siehe "Erstellen und Ändern von Ressourcenimportregeln" auf Seite 209.

Siehe "Manuelles Ausführen von Ressourcenimportregeln" auf Seite 214.

Diese Aufgabe ist ein Schritt beim Importieren von Ressourcen mit Microsoft Active Directory Import.

Siehe "Importieren von Ressourcen mit Microsoft Active Directory-Import" auf Seite 207.

So planen Sie Ressourcenimportregeln

1 Klicken Sie in Symantec Management Console im Menü "Aktionen" auf "Erkennen" > "Microsoft Active Directory importieren".

2 Aktivieren Sie auf der Seite "Microsoft Active Directory-Import" neben der Ressourcenimportregel, die Sie planen möchten, das Kontrollkästchen "Aktiviert".

3 Klicken Sie in der Beschreibung der Ressourcenimportregel auf "Angegebene Zeitpläne".

4 Richten Sie im Fenster "Regelplanung" einen oder beide der folgenden Zeitpläne ein:

Voller Import-Zeitplan	Importiert alle von der Ressourcenimportregel identifizierten Ressourcen.
Zeitplan aktualisieren	Importiert nur die von der Ressourcenimportregel identifizierten neuen und geänderten Ressourcen.

Siehe "So richten Sie einen Zeitplan ein" auf Seite 213.

5 Klicken Sie auf "OK", um die Seite "Regelplanung" zu schließen.

6 Klicken Sie auf "Übernehmen".

So richten Sie einen Zeitplan ein

1 Aktivieren Sie das Kontrollkästchen "Aktivieren" des gewünschten Zeitplans.

2 Wählen Sie in der Dropdown-Liste "Zeitplan" einen der folgenden Zeitpläne aus:

Am/Um	Geben Sie das passende Datum und die passende Uhrzeit an. Wenn Sie möchten, dass sich der Zeitplan wiederholt, aktivieren Sie "Wiederholen alle" und geben anschließend das Wiederholungsintervall an.
Gemeinsam genutzter Zeitplan	Wählen Sie den passenden gemeinsam genutzten Zeitplan aus.

Konfigurieren des Zeitplans für Verzeichnissynchronisierung

Um CMDB mit Active Directory-Ressourcen synchron zu halten, müssen Sie den passenden Zeitplan für die Verzeichnissynchronisierung konfigurieren. Der Zeitplan für die Verzeichnissynchronisierung identifiziert alle vorher importierten Ressourcen, die nicht mehr im Active Directory existieren, und entfernt sie aus CMDB. Er erkennt auch alle Ressourcen, die umbenannt oder außerhalb der Organisationseinheiten verschoben wurden, über die sie zuerst importiert wurden, und löscht die entsprechenden Datensätze aus CMDB.

Warnung: Wenn Sie einen Computer aus einer Domäne in eine Arbeitsgruppe verschieben, müssen Sie den Datensatz des Computers aus Active Directory löschen, um eine Duplizierung in der CMDB zu vermeiden.

Diese Aufgabe ist ein Schritt beim Importieren von Ressourcen mit Microsoft Active Directory-Import.

Siehe "Importieren von Ressourcen mit Microsoft Active Directory-Import" auf Seite 207.

So konfigurieren Sie den Zeitplan für Verzeichnissynchronisierung

1. Klicken Sie in Symantec Management Console im Menü "Aktionen" auf "Erkennen" > "Microsoft Active Directory importieren".
2. Aktivieren Sie auf der Seite "Microsoft Active Directory-Import" unter "Zeitplan für Verzeichnissynchronisierung" die Option "Aktiviert".
3. Wählen Sie in der Dropdown-Liste "Zeitplan" einen der folgenden Zeitpläne aus:

Am/Um	Geben Sie das passende Datum und die passende Uhrzeit an. Wenn Sie möchten, dass sich der Zeitplan wiederholt, aktivieren Sie "Wiederholen alle" und geben anschließend das Wiederholungsintervall an.
Gemeinsam genutzter Zeitplan	Wählen Sie den passenden gemeinsam genutzten Zeitplan aus.

4. Klicken Sie auf "Übernehmen".

Manuelles Ausführen von Ressourcenimportregeln

Wenn Sie bestimmte Ressourcen sofort importieren müssen, können Sie die geeignete Ressourcenimportregel manuell ausführen. Sie können die Ressourcenimportregel als vollständigen Import oder Update-Import ausführen. Das manuelle Ausführen einer Ressourcenimportregel hat keine Auswirkung auf den Zeitplan, falls einer aktiviert ist.

Siehe "Planen von Ressourcenimportregeln" auf Seite 212.

Diese Aufgabe ist ein Schritt beim Importieren von Ressourcen mit Microsoft Active Directory-Import.

Siehe "Importieren von Ressourcen mit Microsoft Active Directory-Import" auf Seite 207.

So führen Sie Ressourcenimportregeln manuell aus

1. Klicken Sie in Symantec Management Console im Menü "Aktionen" auf "Erkennen" > "Microsoft Active Directory importieren".
2. Wählen Sie auf der Seite "Microsoft Active Directory-Import" die Ressourcenimportregel aus, die Sie ausführen möchten.
3. Klicken Sie auf eine der folgenden Optionen:

Ausgewählte Importregel jetzt ausführen (vollständiger Import)	Führt einen vollständigen Import der ausgewählten Ressourcenimportregel aus.
Ausgewählte Importregel jetzt ausführen (aktualisierter Import)	Führt einen Update-Import der ausgewählten Ressourcenimportregel aus.

4. Wenn Sie den Importprozess aus einem bestimmten Grund beenden möchten, klicken Sie auf "Stopp".

Kapitel 13

Erkennen von Netzwerkgeräten

In diesem Kapitel werden folgende Themen behandelt:

- Info zu Network Discovery
- Erkennen von Netzwerkgeräten
- Delegieren von Netzwerkerkennungsaufgaben an Nicht-Administratorbenutzer
- Importieren von MIB-Dateien

Info zu Network Discovery

Mithilfe der Option "Network Discovery" können Sie alle IP-Geräte erkennen, die eine Verbindung zu Ihrem Netzwerk hergestellt haben. Mit "Network Discovery" können Sie neue Netzwerkgeräte und auch jene finden, deren Erkennungseigenschaften geändert wurden.

Network Discovery ist Teil von Symantec Management-Plattform.

"Network Discovery" kann Router, Switches, Hubs, Netzwerkdrucker, Novell NetWare-Server und die Computer erkennen, auf denen Windows, UNIX, Linux und Macintosh ausgeführt werden. Sie können eine Vielzahl von Protokollen zur Erkennung von Geräten verwenden, wie beispielsweise AMT, SNMP, WMI und andere.

Die erfassten Informationen können Ihnen bei der Ausführung folgender Schritte hilfreich sein:

- Planen für Imaging
- Aktualisieren der Treiber für bestimmte Hardwaretypen

- Konfigurieren der Änderungen an Routern oder Switches
- Identifizieren der Computer, auf denen die Betriebssysteme ausgeführt werden, die von Symantec Management-Agent derzeit nicht unterstützt werden

Sie können Kategorien auch aktualisieren, damit die neuen Geräte, die zum Netzwerk hinzugefügt werden, während der Suche identifiziert werden können.

Da "Network Discovery" in Symantec Management-Plattform integriert ist, werden erkannte Geräte automatisch als Ressourcen in der zentralen Datenbank der Plattform (CMDB) erstellt. Mithilfe der Task Management-Komponente der Plattform können Sie die Ausführung von Erkennungsaufgaben entsprechend planen, wenn es für Ihre Anforderungen optimal ist.

Siehe "Erkennen von Netzwerkgeräten" auf Seite 217.

Siehe "Delegieren von Netzwerkerkennungsaufgaben an Nicht-Administratorbenutzer" auf Seite 229.

Sie können Windows-basierte Computer über Domänen erkennen oder über Microsoft Active Directory importieren.

Siehe "Ressourcenerkennungsmethoden" auf Seite 198.

Erkennen von Netzwerkgeräten

Um Ihr Netzwerk erfolgreich verwalten zu können, müssen Sie die verschiedenen Geräte im Netzwerk identifizieren. Network Discovery erkennt neue Netzwerkgeräte sowie Netzwerkgeräte, deren Erkennungseigenschaften geändert wurden, und identifiziert früher erkannte Netzwerkgeräte, die nicht mehr vorhanden sind. Für die Erkennung werden Geräteerkennungsaufgaben durchgeführt und die Daten werden dem Notification Server gemeldet. Die Geräteerkennungsdaten werden als bekannte Ressourcen in der Configuration Management Database (CMDB) gespeichert. Sie können Ihre Erkennungsdaten auf dem aktuellen Stand halten, indem Sie regelmäßig automatische Erkennungsaufgaben ausführen lassen.

Sie können alle Geräte im Netzwerk erkennen und in die CMDB eingeben.

Siehe "Info zu Network Discovery" auf Seite 216.

Tabelle 13-1 Prozess für das Erkennen von Netzwerkgeräten

Schritt	Aktion	Beschreibung
Schritt 1	(Optional) Konfigurieren von "Network Discovery"-Optionen	Sie können Standardoptionen für Aufgaben und SNMP-Klassifikationen konfigurieren. Siehe "Konfigurieren von Erkennungseinstellungen" auf Seite 218.

Schritt	Aktion	Beschreibung
Schritt 2	Erstellen einer "Network Discovery"-Aufgabe	Sie können eine Aufgabe erstellen und planen, um entweder ein einzelnes Gerät oder mehrere Geräte in einem Netzwerk zu erkennen. Sie können zwei Methoden für das Erstellen von Aufgaben verwenden: Mithilfe des "Network Discovery"-Assistenten oder durch manuelles Erstellen von Aufgaben Siehe "Erstellen von "Network Discovery"-Aufgaben mithilfe des Assistenten" auf Seite 220. Siehe "Manuelles Erstellen und Ändern von Network Discovery-Aufgaben" auf Seite 221.
Schritt 3	(Optional) Ändern der Aufgabeneinstellungen oder Zeitpläne	Nachdem Sie die Aufgabe "Network Discovery" erstellt haben, können Sie die Aufgabeneinstellungen ändern oder zusätzliche Zeitpläne hinzufügen. Siehe "Manuelles Erstellen und Ändern von Network Discovery-Aufgaben" auf Seite 221.
Schritt 4	Anzeigen von Erkennungsdaten	Sie können den Status der "Network Discovery"-Aufgaben und Berichte mit Erkennungsergebnissen anzeigen. Siehe "Anzeigen erkannter Geräte in Organisationsansichten" auf Seite 227. Siehe "Anzeigen von Erkennungsberichten" auf Seite 227.
Schritt 5	Klassifizieren unbekannter Geräte	Wenn Sie über Geräte mit einer unbekannten Klassifizierung verfügen, können Sie die SNMP-Klassifizierungsliste ändern. Siehe "Klassifizieren von SNMP-Geräten " auf Seite 228.

Konfigurieren von Erkennungseinstellungen

Für Network Discovery-Aufgaben können Sie globale Einstellungen konfigurieren. Diese Einstellungen werden verwendet, sobald eine neue Aufgabe erstellt wird.

Sie können Network Discovery auf folgende Weisen konfigurieren:

Einstellungen für Erkennungsaufgaben	In den Einstellungen "Network Discovery" können Sie die maximale Anzahl der Threads pro Erkennungsaufgabe festlegen. Während des Erkennungsvorgangs wird ein separater Thread für jedes Gerät verwendet. Diese Anzahl ist die Standard-Maximalzahl von Threads, wenn eine neue Network Discovery-Aufgabe erstellt wird. Außerdem können Sie diese Anzahl für individuelle Aufgaben konfigurieren, indem Sie die erweiterten Eigenschaften der Aufgabe bearbeiten. Wenn die Erkennungsaufgaben den Server stark belasten, ist es sinnvoll, diesen Wert zu verringern.
SNMP-Geräteklassifikation	Wenn Sie SNMP-Geräte erkennen, können Sie eine Netzwerkgeräteklassifikation mit der Ressource identifizieren. Mit dieser Methode können Sie Ressourcen als Router, Switches, Drucker, Server usw. identifizieren. Sie können die Klassifizierungen für erkannte SNMP-Ressourcen konfigurieren. Siehe "Klassifizieren von SNMP-Geräten " auf Seite 228.

Diese Aufgabe ist ein Schritt beim Erkennen von Netzwerkgeräten.

Siehe "Erkennen von Netzwerkgeräten" auf Seite 217.

So konfigurieren Sie Erkennungseinstellungen

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster "Einstellungen > Erkennung und Inventarisierung" und klicken Sie dann auf "Network Discovery-Einstellungen".
3. Geben Sie auf der Seite "Network Discovery-Einstellungen" die Höchstzahl Threads pro Verteilungsaufgabe ein.

   Während des Erkennungsvorgangs wird ein separater Thread für jedes Gerät verwendet.

   Diese Anzahl ist die Standard-Maximalzahl von Threads, wenn eine neue Network Discovery-Aufgabe erstellt wird. Außerdem können Sie diese Anzahl für individuelle Aufgaben konfigurieren, indem Sie die erweiterten Eigenschaften der Aufgabe bearbeiten.

   Wenn die Erkennungsaufgaben den Server stark belasten, ist es sinnvoll, diesen Wert zu verringern.
4. Klicken Sie auf "Änderungen speichern".

Erstellen von "Network Discovery"-Aufgaben mithilfe des Assistenten

Der Network Discovery-Assistent ist ein Administratortool, das Sie durch das Erstellen einer Erkennungsaufgabe und das Konfigurieren von Einstellungen führt. Sie können die erweiterten Einstellungen und Zeitpläne der Aufgabe bearbeiten.

Diese Aufgabe ist ein Schritt beim Erkennen von Netzwerkgeräten.

Siehe "Erkennen von Netzwerkgeräten" auf Seite 217.

So erstellen Sie Network Discovery-Aufgaben mit dem Network Discovery-Assistenten

1. Wählen Sie in der Symantec Management Console im Menü "Startseite" die Option "Erkennung und Inventarisierung > Network Discovery".
2. Klicken Sie im Web-Part "Schnellstartaktionen für Network Discovery" auf "Erkennungsassistenten starten".
3. Wählen Sie im Assistenten eine Erkennungsmethode aus, und klicken Sie anschließend auf "Weiter".

   Siehe "Methoden zum Erkennen von Netzwerkgeräten" auf Seite 224.
4. Geben Sie die Bereiche des zu erkennenden Netzwerks an, und klicken Sie anschließend auf "Weiter".

   Siehe "Info zum Auswählen von zu erkennenden Netzwerkbereichen" auf Seite 226.
5. Wählen Sie ein Verbindungsprofil aus, und klicken Sie anschließend auf "Weiter".

   Verbindungsprofile legen die zur Erkennung zu verwendenden Protokolle fest. Sie können ein bestehendes Profil verwenden oder ein neues erstellen.

   Siehe "Erstellen von Verbindungsprofilen mit Network Discovery" auf Seite 222.

   Siehe "Erstellen oder Duplizieren eines Verbindungsprofils" auf Seite 223.
6. Benennen Sie die Aufgabe, und klicken Sie anschließend auf "Weiter".
7. Planen Sie die Aufgabe, und klicken Sie anschließend auf "Fertig stellen".

   Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.
8. Die vom Erkennungsassistenten erstellten Aufgaben werden unten auf der Seite "Network Discovery - Startseite" angezeigt.

   Sie müssen evtl. auf das Symbol zum Aktualisieren klicken, damit neu erstellte Aufgaben angezeigt werden.

Manuelles Erstellen und Ändern von Network Discovery-Aufgaben

Sie können Aufgaben manuell über das Task Management-Portal erstellen und ändern. Mit dieser Option können Sie erweiterte Optionen und Zeitpläne konfigurieren. Wenn Sie Aufgaben manuell erstellen, können Sie ein Netzwerk oder einzelne Geräte erkennen.

Diese Aufgabe ist ein Schritt beim Erkennen von Netzwerkgeräten.

Siehe "Erkennen von Netzwerkgeräten" auf Seite 217.

So erstellen Sie eine Aufgabe zur Netzwerkerkennung manuell

1. Führen Sie in Symantec Management Console einen der folgenden Schritte aus:
   - Wählen Sie im Hauptmenü die Option "Erkennung und Inventarisierung > Netzwerkerkennung" und klicken Sie dann im Web-Part "Netzwerkerkennung - Aufgabenmanagement" auf der Registerkarte "Verfügbare Aufgaben" auf "Neu".
   - Klicken Sie im Menü "Verwaltung" auf "Aufträge und Aufgaben". Erweitern Sie im linken Teilfenster den Eintrag "Systemaufträge und -aufgaben", klicken Sie mit der rechten Maustaste auf "Erkennung und Inventarisierung" und wählen Sie dann im Kontextmenü die Option "Neu > Aufgabe". Klicken Sie im Dialogfeld "Neue Aufgabe erstellen" im linken Teilfenster unter "Erkennung und Inventarisierung" auf "Netzwerk erkennen".
2. Geben Sie der Aufgabe einen eindeutigen und aussagekräftigen Namen.
3. Wählen Sie ein Verbindungsprofil aus.

   Verbindungsprofile legen die zur Erkennung zu verwendenden Protokolle fest. Sie können ein bestehendes Profil verwenden oder ein neues erstellen.

   Siehe "Erstellen von Verbindungsprofilen mit Network Discovery" auf Seite 222.

   Siehe "Erstellen oder Duplizieren eines Verbindungsprofils" auf Seite 223.
4. Wählen Sie eine Erkennungsmethode aus.

   Siehe "Methoden zum Erkennen von Netzwerkgeräten" auf Seite 224.
5. Geben Sie die Bereiche des zu erkennenden Netzwerks an.

   Siehe "Info zum Auswählen von zu erkennenden Netzwerkbereichen" auf Seite 226.
6. (Optional) Um die maximale Anzahl der gleichzeitig zu erkennenden Geräte zu konfigurieren, klicken Sie auf "Erweitert".
7. Klicken Sie auf "OK".

8 Planen Sie die Aufgabe im daraufhin angezeigten Fenster.

Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.

9 Wählen Sie zum Anzeigen der Aufgabe im linken Teilfenster "Aufträge und Aufgaben > Systemaufträge und -aufgaben > Erkennung und Inventarisierung". Sie müssen evtl. auf das Symbol zum Aktualisieren klicken, um neu erstellte Aufgaben anzuzeigen.

So erstellen Sie manuell eine Aufgabe zur Erkennung eines einzelnen Geräts

1 Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Aufträge und Aufgaben". Erweitern Sie im linken Teilfenster den Eintrag "Systemaufträge und -aufgaben", klicken Sie mit der rechten Maustaste auf "Erkennung und Inventarisierung" und wählen Sie im Kontextmenü die Option "Neu > Aufgabe".

2 Klicken Sie im Dialogfeld "Neue Aufgabe erstellen" im linken Teilfenster unter "Erkennung und Inventarisierung" auf "Gerät erkennen".

3 Geben Sie der Aufgabe einen eindeutigen und aussagekräftigen Namen.

4 Wählen Sie ein Verbindungsprofil aus.

Verbindungsprofile legen die zur Erkennung zu verwendenden Protokolle fest. Sie können ein bestehendes Profil verwenden oder ein neues erstellen.

Siehe "Erstellen von Verbindungsprofilen mit Network Discovery" auf Seite 222.

Siehe "Erstellen oder Duplizieren eines Verbindungsprofils" auf Seite 223.

5 Klicken Sie auf "OK", um die Aufgabe zu speichern.

6 Klicken Sie im daraufhin angezeigten Fenster auf "Neuer Zeitplan".

7 Planen Sie im Dialogfeld "Neuer Zeitplan" die Aufgabe, geben Sie das zu erkennende Gerät an, indem Sie die IP-Adresse oder den Namen eingeben, und klicken Sie dann auf "Zeitplan".

Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.

8 Wählen Sie zum Anzeigen der Aufgabe im linken Teilfenster "Aufträge und Aufgaben > Systemaufträge und -aufgaben > Erkennung und Inventarisierung". Sie müssen evtl. auf das Symbol zum Aktualisieren klicken, damit neu erstellte Aufgaben angezeigt werden.

Erstellen von Verbindungsprofilen mit Network Discovery

Network Discovery-Aufgaben verwenden Verbindungsprofile zum Konfigurieren der zur Kommunikation mit Netzwerkgeräten verwendeten Protokolle.

Verbindungsprofile sind eine Komponente der Symantec Management-Plattform. Die Art, wie Sie Protokolle und Verbindungsprofile verwenden, wirkt sich auf die Geräteerkennungsfähigkeit von Network Discovery aus.

Die Netzwerksuche verwendet Verbindungsprofile, um über die im Profil aktivierten Protokolle eine Verbindung zu den Zielgeräten herzustellen. Wird ein Gerät erkannt, wird in der CMDB eine Ressource für dieses Gerät erstellt. Die Ressource speichert einen Datensatz der Protokolle, die für die Kommunikation mit dem Gerät verwendet wurden.

Wenn an den Verbindungsprofilen Änderungen bezüglich der Protokolle oder der Identifikationsdaten für diese Protokolle vorgenommen werden, und Sie nun Geräte mithilfe dieser geänderten Einstellungen erkennen möchten, müssen Sie die Erkennung erneut ausführen.

Sie können verschiedene Verbindungsprofile erstellen und benutzen, je nach den in Ihrem Netzwerk verwendeten Geräten und Protokollen. Bei der Konfiguration von Network Discovery-Aufgaben können Sie entweder ein bestehendes Verbindungsprofil verwenden oder Ihr eigenes Profil erstellen.

Siehe "Erstellen von "Network Discovery"-Aufgaben mithilfe des Assistenten" auf Seite 220.

Siehe "Manuelles Erstellen und Ändern von Network Discovery-Aufgaben" auf Seite 221.

So erstellen Sie ein Verbindungsprofil

1. Klicken Sie in einer Aufgabe "Netzwerksuche" auf "Neues Verbindungsprofil".

   Alle aufgelisteten Protokolle werden unterstützt.
2. Benennen Sie das Verbindungsprofil.
3. Deaktivieren oder aktivieren Sie die einzelnen Protokolle, konfigurieren Sie die Verwendungseinstellungen und wählen Sie die Identifikationsdaten für die einzelnen Protokolle aus.

   Siehe "Verwalten von Identifikationsdaten" auf Seite 121.
4. Klicken Sie auf "OK".
5. Wählen Sie das Profil aus der Dropdown-Liste aus.

Erstellen oder Duplizieren eines Verbindungsprofils

Verbindungsprofile speichern die Informationen, die erforderlich sind, um mit Computern und anderen Netzwerkgeräten mit Standard-Netzwerküberwachungsprotokollen zu kommunizieren. Zu diesen Protokollen gehören SNMP, WMI, WSMan und einige andere.

Verbindungsprofile werden während des Network Discovery-Vorgangs mit Geräten verknüpft. Während der Erkennung wird ein Verbindungsprofil ausgewählt, um die zu verwendenden Protokolle und Identifikationsdaten zu definieren. Wenn die Erkennung abgeschlossen ist, wird dieses Verbindungsprofil mit jeder erkannten Ressource verknüpft. Wenn Informationen erforderlich sind, wird das verknüpfte Verbindungsprofil verwendet, um eine Verbindung herzustellen.

Üblicherweise sollten Sie für jedes Segment des Netzwerks, für das andere Identifikationsdaten zur Netzwerküberwachung verwendet werden, ein neues Verbindungsprofil erstellen.

So erstellen Sie ein Verbindungsprofil

1. Klicken Sie in Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster "Überwachung und Warnmeldungen > Protokollverwaltung > Verbindungsprofile" und klicken Sie auf "Verbindungsprofile verwalten".
3. Klicken Sie auf der Seite "Verbindungsprofile verwalten" auf "Einstellungen hinzufügen" und geben Sie einen Namen für das neue Profil an.
4. Geben Sie im Dialogfeld "Gruppeneinstellungen definieren" den Namen des neuen Profils ein, aktivieren Sie die gewünschten Protokolle, und stellen die erforderlichen Protokolldetails bereit.

   Klicken Sie oben rechts in jedem zu aktivierenden Protokoll auf den farbigen Kreis und dann auf "Ein".

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.
5. Klicken Sie auf "OK".

Methoden zum Erkennen von Netzwerkgeräten

Beim Erkennen von Netzwerkgeräten können Sie eine der folgenden Erkennungsmethoden verwenden: Ping oder ARP

Siehe "Erkennen von Netzwerkgeräten" auf Seite 217.

Sie starten Erkennungsaufgaben durch den Network Discovery-Assistenten, der auf der Startseite von Network Discovery verfügbar ist. Hier geben Sie an, welche Erkennungsmethode verwendet werden soll.

Siehe "Erstellen von "Network Discovery"-Aufgaben mithilfe des Assistenten" auf Seite 220.

Siehe "Manuelles Erstellen und Ändern von Network Discovery-Aufgaben" auf Seite 221.

Tabelle 13-2 Netzwerkerkennungmethoden

Methode	Beschreibung
Ping	Vorhandene Geräte werden ermittelt, indem eine ICMP-Ping-Anfrage an jede mögliche IP-Adresse in einem angegebenen Bereich oder Subnetz gesendet wird. Wenn ein Gerät einen Ping-Anfrage erhält, reagiert es mit einer Antwort und meldet vorhandene Geräte der Erkennungs-Engine. Sie können diese Methode verwenden, um eine umfassende Suche durchzuführen, die alle Geräte findet. Diese Methode ist unbrauchbar, wenn Ihre Netzwerk-Firewall keine Ping-Anfragen ermöglicht. Diese Methode ist für spärliche Subnetze (jene mit wenigen Geräten in ihrem Adressbereich) unter Umständen nicht optimal. Die Engine benötigt unter Umständen viel Zeit beim Warten auf Antworten von Geräten, die nicht vorhanden sind. Diese Situation tritt auf, weil die Engine wartet, bis das angegebene Zeitlimit abläuft, und die Engine es anschließend einmal oder mehrmals erneut versucht, falls anwendbar.
ARP	Vorhandene Geräte werden erstmalig ermittelt, indem die ARP-Cache-Tabelle eines Netzwerkinfrastrukturgeräts (beispielsweise ein Switch oder Router) gelesen wird. Die ARP-Cache-Tabelle wird vom Gerät gelesen und anschließend wird jedes Gerät in der Tabelle einzeln knotaktiert und erkannt. Diese Erkennungsmethode liefert der Erkennungs-Engine einen Satz zu erkennender Geräten. Jedoch werden ARP-Cache-Tabelleneinträge nach verhältnismäßig kurzer Inaktivität entfernt. Dies bedeutet, dass der Scan selbst keine deaktivierten Geräte berücksichtigt. Sie können dieses Problem beheben, indem Sie eine Ping-Anfrage an jedes Gerät in einem Zielnetzwerk senden. Dieser Prozess aktualisiert die Tabelle, in der alle Geräte enthalten sind.

Info zum Auswählen von zu erkennenden Netzwerkbereichen

Wenn Sie eine Network Discovery-Aufgabe erstellen, identifizieren Sie entweder das einzelne Netzgerät oder Adressbereiche, die erkannt werden sollen. Dazu geben Sie die Adressen, die ein- oder ausgeschlossen werden sollen oder eine Kombination von beiden an.

Siehe "Erstellen von "Network Discovery"-Aufgaben mithilfe des Assistenten" auf Seite 220.

Siehe "Manuelles Erstellen und Ändern von Network Discovery-Aufgaben" auf Seite 221.

Wenn Sie ein Seed-Gerät haben und einen Einschließbereich erstellen, muss das Seed-Gerät im Einschließbereich enthalten sein, damit es erkannt werden kann.

Um einen benutzerdefinierten Bereich zu verwenden, können Sie Platzhalter oder Bereiche von Werten im dritten oder vierten Oktett der Adresse verwenden. Es folgen Beispiele der Verwendung eines benutzerdefinierten Bereichs:

172.16.[*].[*]	Sie können ein Sternchen als Platzhalter verwenden, der für einen Wert zwischen 0 und 254 steht.
172.16.[1-24].[1-254] 172.16.[3-30].[1-10]	Sie können einen Wertebereich angeben. Alle Adressen im Bereich werden aus- oder eingeschlossen.

Sie können auch eine Textdatei importieren, um die Adressen anzugeben, die Sie ein- oder ausschließen möchten. Wenn Sie eine Textdatei konfigurieren, müssen Sie alle Informationen einschließen, die für diesen Typ von Adresse oder Bereich erforderlich sind. Wenn Sie beispielsweise einen IP-Adressbereich angeben, müssen Sie die Start-IP-Adresse, die End-IP-Adresse und die Maske angeben. Sie können auch benutzerdefinierte IP-Adressbereiche in einer Importdatei angeben.

Es folgt ein Beispiel für das Format einer Importdatei:

```
SingleIpAddr, Include, 192.168.0.2,
SingleIpAddr, Exclude, 192.168.0.3,

Hostname, Include, hostname1.company1.com
Hostname, Exclude, hostname2

Subnet, Include, 192.168.0.0, 255.255.255.0
Subnet, Exclude, 192.169.0.0, 255.255.255.0

CustomIpAddrRange, Include, 192.168.*.*, 255.255.0.0
CustomIpAddrRange, Exclude, 10.192.1-25.1-254, 255.0.0.0
```

```
CustomIpAddrRange, Include, 10.192.4.1-100, 255.255.254.0

IpAddrRange, Include, 192.168.0.1, 192.168.0.200, 255.255.255.0
IpAddrRange, Exclude, 192.168.0.120, 192.168.1.140, 255.255.255.0
```

Anzeigen erkannter Geräte in Organisationsansichten

Wenn ein Gerät erkannt wird, wird automatisch eine Ressource dafür in der Configuration Management Database (CMDB) erstellt. Sie können die Geräte in Organisationsübersichten anzeigen. Organisationsübersichten zeigen alle bekannten Ressourcen in Ihrer Umgebung. Sie können alle erkannten Geräte in einer Übersicht anzeigen: Netzwerkressourcen. Außerdem gibt es Übersichten für bestimmte Ressourcentypen, wie z. B. Computer, Netzwerkdrucker usw.

Wenn der Ressourcentyp des Geräts nicht bekannt ist, wird Ressourcentyp als Eigenschaft der Ressource angezeigt. Bei Geräten mit dem Ressourcentyp "Netzwerkressource" ist der Gerätetyp unbekannt. Diese unbekannten Geräte werden in der Netzwerkressourcenübersicht angezeigt, nicht jedoch in den einzelnen Ressourcentypenübersichten. Wenn Sie über Geräte mit einer unbekannten Klassifizierung verfügen, können Sie die SNMP-Klassifizierungsliste ändern.

Siehe "Klassifizieren von SNMP-Geräten " auf Seite 228.

Diese Aufgabe ist ein Schritt beim Vorgang zum Erkennen von Netzwerkgeräten.

Siehe "Erkennen von Netzwerkgeräten" auf Seite 217.

So zeigen Sie erkannte Geräte in Organisationsansichten an

1. Klicken Sie in Symantec Management Console im Menü "Verwaltung" auf "Alle Ressourcen".
2. Im linken Teilfenster erweitern Sie "Standard > Alle Ressourcen > Asset" und klicken Sie auf "Netzwerkressource".
3. Zum Anzeigen einer bestimmten Ressource klicken Sie im linken Teilfenster unter "Netzwerkressource" auf einen Ressourcentyp.

Anzeigen von Erkennungsberichten

Sie können die Ergebnisse der Erkennung in Berichten anzeigen. Es stehen vordefinierte Berichte zur Auswahl; Sie können aber auch eigene Berichte erstellen.

Im Bericht "Erkannte Geräte" können Sie die auf einem Datumsbereich, der Erkennungsmethode, dem verwendeten Protokoll oder der verwendeten Aufgabe basierenden Ergebnisse filtern.

Im Bericht "Erkannte Geräte nach Gruppe" können Sie die auf einem Datumsbereich, der Erkennungsmethode, dem verwendeten Protokoll, der verwendeten Aufgabe oder dem Gerätetyp basierenden Ergebnisse gruppieren.

Diese Aufgabe ist ein Schritt beim Erkennen von Netzwerkgeräten.

Siehe "Erkennen von Netzwerkgeräten" auf Seite 217.

So zeigen Sie Erkennungsberichte an

1. Wählen Sie in der Symantec Management Console im Menü "Berichte" die Option "Alle Berichte".
2. Erweitern Sie im linken Teilfenster "Berichte > Erkennung und Inventarisierung" und klicken Sie dann auf den gewünschten Bericht.
3. Geben Sie die Parameter für den Bericht ein und klicken Sie auf "Aktualisieren".

   Siehe "Infos zu Notification Server-Berichten" auf Seite 460.

Klassifizieren von SNMP-Geräten

Erkannte SNMP-Geräte werden anhand ihres Gerätetyps identifiziert, wie z. B. Computer, Netzwerkdrucker usw. Zur Identifizierung des Gerätetyps muss Network Discovery die SNMP-Geräteklassifizierung dieses Typs kennen. Network Discovery enthält eine vordefinierte Liste geläufiger SNMP-Geräte. Wenn das erkannte Gerät auf der Liste ist, kann es identifiziert werden. Wenn ein Gerät nicht in der Liste ist, wird es mit dem generischen Ressourcentyp "Netzwerkressource" bezeichnet.

Sie können die vordefinierte Liste auf der Seite "Geräteklassifizierung" einsehen. Diese Seite enthält die Klassifizierungen geläufiger Geräte. Diese Daten enthalten die SNMP-Objektkennung, den Gerätetyp, den Hersteller und das Gerätemodell. Wenn die erkannte SNMP-Objektkennung mit einem Objekt aus der Liste übereinstimmt, werden die entsprechenden Daten eingetragen.

Sie können vor dem Ausführen von Network Discovery-Aufgaben die Geräteklassifizierungsliste ansehen, die verbreitete Hersteller umfasst. Wenn die Liste unvollständig ist, können Sie Klassifizierungen hinzufügen oder bearbeiten, um die Liste an Ihre Umgebung anzupassen. Es lohnt sich, die Geräteklassifizierungsliste durchzugehen und anzupassen, da so genauere Erkennungsdaten erzielt werden. Diese Aufgabe ist für die Erkennung jedoch nicht erforderlich. Sie können sie auch nach der Erkennung durchführen, müssen die Erkennung jedoch dann erneut durchlaufen lassen, um die aktualisierten Klassifizierungen zu erhalten.

Wenn Sie die Informationen für eine vorhandene SNMP-Geräteklassifizierung ändern, müssen Sie jedes Gerät erneut scannen, das vorher unter Verwendung dieses Eintrags klassifiziert wurde. Das erneute Scannen ist notwendig, damit die Geräte mit geänderten Informationen erneut klassifiziert werden.

Nach Ausführung einer Network Discovery-Aufgabe können Sie Geräte mit unbekannter Klassifzierung haben. Wenn die Objektkennung für diese Geräte bekannt ist, können Sie sie zur Klassifizierungsliste hinzufügen. Bei der nächsten Ausführung der Network Discovery-Aufgabe werden diese Geräte dann anhand der aktuelleren Liste klassifiziert.

Sie können die zur Identifizierung von SNMP-Geräten verwendeten SNMP-Geräteklassifizierungswerte konfigurieren. Network Discovery enthält eine Liste gebräuchlicher Geräte. Sie können Klassifizierungen hinzufügen, bearbeiten oder entfernen, um die Liste an Ihre Netzwerkumgebung anzupassen. Nachdem Sie eine Geräteklassifikation ändern, müssen Sie sie erneut erkennen, damit sie erneut klassifiziert werden kann.

Diese Aufgabe ist ein Schritt beim Vorgang zum Erkennen von Netzwerkgeräten.

Siehe "Erkennen von Netzwerkgeräten" auf Seite 217.

So klassifizieren Sie SNMP-Geräte

1. Klicken Sie in der Symantec Management Console im Menü "Startseite" auf "Erkennung und Inventarisierung > Network Discovery".
2. Klicken Sie unter "Schnellstartaktionen für Network Discovery" auf "SNMP-Geräteklassifizierung".
3. Um eine neue Klassifizierung hinzuzufügen, klicken Sie auf "Hinzufügen" und geben Sie die Daten Ihres Geräts ein.

   Die SNMP-Objektkennung muss ein eindeutiger Wert sein, der vom Gerätehersteller kommt.
4. Sie können auch Klassifizierungen bearbeiten oder entfernen, um die Liste an Ihre Netzwerkumgebung anzupassen.
5. Zur Neuklassifizierung von Geräten basierend auf neuen Einstellungen müssen Sie die Erkennung erneut ausführen.

Delegieren von Netzwerkerkennungsaufgaben an Nicht-Administratorbenutzer

Als Netzwerkadministrator arbeiten Sie möglicherweise in einem Team mit anderen Administratoren, an die Sie bestimmte Aufgaben zur Netzwerkverwaltung delegieren können. Unabhängig davon, ob Sie alleine oder in einem Team von Administratoren arbeiten, Sie müssen unter Umständen Network Delivery-Aufgaben an andere Benutzer bzw. Nicht-Administratoren delegieren.

Network Discovery-Aufgaben erfordern Privilegien für das Arbeiten mit Verbindungsprofilen und Identifikationsdaten. Diese Privilegien werden durch eine

Kombination von Berechtigungen und Privilegien gewährt. Berechtigungen werden standardmäßig Elementen wie beispielsweise Dateien, Aufgaben und Assistenten zugewiesen. Privilegien werden Benutzerrollen gewährt, u. a. der vordefinierten Administratorrolle und den vordefinierten Nicht-Administrator-Rollen. Der Schnittpunkt zwischen Elementberechtigungen und Rollenprivilegien legt fest, was Administratoren und Nicht-Administratoren mit Elementen tun können.

Siehe "Info zu Network Discovery" auf Seite 216.

Jede der vordefinierten Nicht-Administratorrollen in der Symantec Management-Plattform enthält vererbte Privilegien.

Siehe "Vordefinierte Sicherheitsrollen" auf Seite 112.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Um es Benutzern zu ermöglichen, Netzwerkgeräte zu erkennen und mit Verbindungsprofilen und Identifikationsdaten zu arbeiten, weisen Sie Benutzerrollen Rechte zu, die es jenen Rollen ermöglichen, Verbindungsprofile und Identifikationsdaten zu erstellen. Dann wählen Sie eine Nicht-Administrator-Benutzerrolle aus, der Sie Benutzer zuweisen. Anschließend begrenzen oder vergrößern Sie den Bereich der Rolle, indem Sie bestimmte Privilegien entfernen oder zuweisen. Um Network Discovery-Aufgaben zu erstellen und auszuführen, muss die Benutzerrolle Zugriff auf mindestens ein Standardverbindungsprofil haben. Dieses Profil kann das Standardverbindungsprofil sein.

Die Rolle "Symantec Vorgesetzte" ist eine Nicht-Administrator-Rolle der höheren Ebene. Anderen Mitarbeitern kann eine Rolle mit begrenzten, dazu gehörenden Rechten zugewiesen werden. Die Rollen "Symantec Mitarbeiter Stufe 1" und "Symantec Mitarbeiter Stufe 2" sind gute Beispiele. Diese Rollen werden in einiger der Aufgaben verwendet, die im Prozess enthalten sind, der in diesem Thema definiert wird. Sie sind nicht auf diese Rollen beschränkt. Es sind vordefinierte Rollen, die für Administratoren am nützlichsten sind.

Sie können mehr als einer Benutzerrolle Aufgaben zuweisen. Ein Benutzer muss Mitglied einer Sicherheitsrolle sein, die über das Privileg "Erkennungsaufgabenverwaltung" verfügt, um Aufgaben erstellen, bearbeiten oder ausführen zu können.

Die Standardrolle "Symantec Vorgesetzte" umfasst mehr Zugriff auf Network Discovery als andere Nicht-Administrator-Rollen. Das Delegieren von Aufgaben an die Rolle "Symantec Vorgesetzte" ist weniger kompliziert als das Delegieren von Aufgaben an Rollen, die keinen Zugriff auf die Durchführung beliebiger Network Discovery-Aufgaben haben.

Wählen Sie eine Rolle aus, an die Aufgaben auf der Basis dessen delegiert werden sollen, was Sie Nicht-Administratoren tun lassen möchten. Delegieren Sie Aufgaben

durch Ausführen jedes Prozessschritts der Reihenfolge nach. Aufgaben, die in späteren Schritten aufgelistet werden, sind möglicherweise von den Rechten abhängig, die in den vorangegangenen Schritten gewährt wurden.

Tabelle 13-3 Prozess für die Delegierung von Netzwerkerkennungsaufgaben an Nicht-Administratorbenutzer

Schritt	Aufgabe	Beschreibung
Schritt 1	Hinzufügen von Nicht-Administratoren zu Sicherheitsrollen, um Network Discovery-Aufgaben durchzuführen	Sie müssen diesen Rollen Benutzer zuweisen, um Aufgaben an Benutzer mit Nicht-Administrator-Rollen zuweisen zu können. Siehe "Hinzufügen von Nicht-Administratorbenutzern zu den Sicherheitsrollen für die Ausführung von Netzwerkerkennungsaufgaben" auf Seite 233.
Schritt 2	Ermöglichen, dass Nicht-Administrator-Rollen Network Discovery-Aufgaben erstellen oder ausführen können	Sie können Network Discovery-Aufgaben an Nicht-Administrator-Rollen delegieren und Nicht-Administrator-Benutzer diesen Rollen zuweisen. Mehrere Standardrollen sind in der Symantec Management-Plattform enthalten, wobei jede Rolle bestimmte dazu gehörende Rechte hat. Die Rolle "Symantec Vorgesetzte" kann Network Discovery-Aufgaben ausführen. Andere Nicht-Administrator-Rollen können nicht einmal vorhandene Aufgaben ausführen, solange Sie der Rolle die erforderlichen Rechte nicht gewähren. Sie müssen bestimmte Schritte durchführen, um es Nicht-Administrator-Rollen zu ermöglichen, Network Discovery-Aufgaben zu erstellen und auszuführen. Standardmäßig können die Rollen "Administratoren", "Symantec Vorgesetzte" und "Symantec Mitarbeiter Stufe 1" bzw. "Symantec Mitarbeiter Stufe 2" die Network Discovery-Portalseite anzeigen. Diese Seite ist ein geeigneter Standort, von dem aus Administratoren Network Discovery-Aufgaben anzeigen und ausführen können. Die Rollen "Administratoren" und "Vorgesetzte" können alle Teile dieser Seite standardmäßig anzeigen. Jedoch wird der Web-Part für "Netzwerkerkennung - Aufgabenmanagement" für andere Benutzer deaktiviert. Damit dieser Web-Part anderen Nicht-Administratorbenutzer angezeigt wird und sie ihn verwenden können, weisen Sie sie einer Sicherheitsrolle zu, für die das Privileg "Erkennungsaufgabenverwaltung" aktiviert wurde. Siehe "Vordefinierte Sicherheitsrollen" auf Seite 112. Siehe "Ermöglichen, dass Nicht-Administratorrollen Netzwerkerkennungsaufgaben erstellen oder ausführen können" auf Seite 235.

Schritt	Aufgabe	Beschreibung
Schritt 3	(Optional aber empfohlen) Gewähren Sie Nicht-Administratorrollen Rechte zum Erstellen von Identifikationsdaten und Verbindungsprofile.	Einer Nicht-Administrator-Rolle können Privilegien zur Erkennung von Netzwerkgeräten sowie zur Erstellung oder Bearbeitung von Identifikationsdaten und Verbindungsprofilen gewährt werden. Das Erstellen oder Bearbeiten von Identifikationsdaten und Verbindungsprofilen ist möglicherweise zur Durchführung der Aufgaben erforderlich, die später in diesem Prozess aufgelistet werden. Dieser Schritt ist optional, weil Benutzer Network Discovery-Aufgaben ohne diese Rechte erstellen können. Sie müssten einfach vorhandene Verbindungsprofile verwenden, auf die sie Zugriff haben. Siehe "Sicherheitsprivilegkategorien" auf Seite 510. Siehe "Gewähren von Privilegien zur Erstellung von Identifikationsdaten und Verbindungsprofilen für Nicht-Administratorrollen" auf Seite 238.
Schritt 4	Erteilen Sie Nicht-Administrator-Rollen Zugriff auf das Standardverbindungsprofil.	Um Network Discovery-Aufgaben zu erstellen und auszuführen, muss eine Benutzerrolle Zugriff auf das Standardverbindungsprofil (oder ein anderes Verbindungsprofil, aber mindestens eines) haben. Siehe "Erteilen von Zugriff für Nicht-Administrator-Rollen auf das Standardverbindungsprofil" auf Seite 239.
Schritt 5	Aktivieren Sie andere Rollen als vordefinierte Sicherheitsrollen, um Aufgaben unter Verwendung des Network Discovery-Assistenten zu erstellen und auszuführen.	Die folgenden Sicherheitsrollen sind vordefiniert und können standardmäßig Aufgaben unter Verwendung des Network Discovery-Assistenten erstellen und ausführen: ■ Administrator ■ Symantec-Supervisor ■ Symantec Mitarbeiter Stufe 2 ■ Symantec Mitarbeiter Stufe 1 Wenn andere Rollen Aufgaben unter Verwendung des Assistenten erstellen und ausführen können sollen, müssen Sie ihnen ausdrücklich den entsprechenden Zugriff erteilen. Siehe "Aktivieren der Erstellung und Ausführung von Aufgaben durch andere Rollen als die vordefinierten Sicherheitsrollen mithilfe des Network Discovery-Assistenten" auf Seite 240.
Schritt 6	(Optional) Aktivieren Sie für ein Verbindungsprofil den Schreibschutz.	Wenn eine bestimmte Nicht-Administratorrolle ein Verbindungsprofil anzeigen, aber nicht bearbeiten können soll, können Sie den Schreibschutz für das Profil aktivieren. Siehe "Aktivieren des Schreibschutzes für ein Verbindungsprofil" auf Seite 242.

Hinzufügen von Nicht-Administratorbenutzern zu den Sicherheitsrollen für die Ausführung von Netzwerkerkennungsaufgaben

Wenn Sie Network Discovery-Aufgaben an Nicht-Administrator-Benutzer delegieren möchten, müssen diese die erforderlichen Privilegien haben, um die betreffenden Aufgaben durchzuführen. Privilegien werden Benutzerrollen zugewiesen. Wenn Sie noch keinen Windows-Benutzer erstellt haben, der Network Discovery-Aufgaben ausführen kann, müssen Sie diesen Benutzer zunächst erstellen. Fügen Sie den Benutzer anschließend der gewünschten Sicherheitsrolle hinzu oder erstellen Sie eine benutzerdefinierte Rolle. Gewähren Sie der Sicherheitsrolle abschließend Privilegien. Danach können Sie die Aufgaben delegieren, für deren Ausführung die Rolle genügend Privilegien hat.

Die Portalseite "Network Discovery" ist ein geeigneter Ort, um Erkennungsaufgaben anzuzeigen und durchzuführen. Administratoren und Symantec-Supervisors haben standardmäßig vollen Zugriff auf diese Seite. Benutzer in anderen, Nicht-Administrator-Rollen können diese Seite anzeigen. Jedoch ist der Web-Part "Erkennungsaufgabenverwaltung" deaktiviert, es sei denn, Sie aktivieren ihn mit der "Berechtigung für die Erkennungsaufgabenverwaltung". Indem Sie Nicht-Administratoren zu Sicherheitsrollen hinzufügen und ihnen Rechte für die Network Discovery-Aufgabenverwaltung gewähren, ermöglichen Sie es ihnen, diese Seite anzuzeigen und zu bearbeiten.

Siehe "Ermöglichen, dass Nicht-Administratorrollen Netzwerkerkennungsaufgaben erstellen oder ausführen können" auf Seite 235.

Symantec Management-Plattform enthält standardmäßig einige vordefinierte Nicht-Administrator-Sicherheitsrollen. Außerdem können Sie benutzerdefinierte Sicherheitsrollen erstellen.

Siehe "Vordefinierte Sicherheitsrollen" auf Seite 112.

Siehe "Erstellen und Konfigurieren von Benutzerkonten der Symantec Management-Plattform" auf Seite 233.

Diese Aufgabe ist ein Schritt im Prozess für die Delegierung von Netzwerkerkennungsaufgaben an Nicht-Administratoren.

Siehe "Delegieren von Netzwerkerkennungsaufgaben an Nicht-Administratorbenutzer" auf Seite 229.

So fügen Sie Nicht-Administratorbenutzer Sicherheitsrollen für die Ausführung von Netzwerkerkennungsaufgaben hinzu

1. Loggen Sie sich bei der Symantec Management Console als Administrator ein.
2. Um einen neuen Windows-Benutzer herzustellen, führen Sie folgende Schritte durch:
   - Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Sicherheit > Kontoverwaltung".
   - Klicken Sie im linken Teilfenster auf "Konten".
   - Klicken Sie auf der Seite "Konten" auf "Hinzufügen".
   - Geben Sie im Dialogfeld "Neues Konto" einen Namen für den neuen Benutzer ein und klicken Sie auf "OK".
   - Geben Sie im rechten Teilfenster auf der Registerkarte "Allgemein" unter "Accountdetails" im Feld "Vollständiger Name" den vollständigen Namen des Benutzers ein.
     Sie können das -Feld "E-Mail" leer lassen. Es ist für dieses Verfahren nicht erforderlich.
   - Klicken Sie unter "Identifikationsdaten" auf "Identifikationsdaten hinzufügen > "Windows".
   - Geben Sie im Dialogfeld "Windows-Identifikationsdaten" den Login-Namen ein, der dem Windows-Benutzer entspricht, der diesem neuen Konto zugeordnet ist und klicken Sie auf "OK" klickt auf.
   - Aktivieren Sie das Konto.
     Klicken Sie oben rechts auf der Seite auf den farbigen Kreis und dann auf "Ein".
3. Um den Benutzer einer Sicherheitsrolle hinzuzufügen. an die Sie Aufgaben delegieren möchten, führen Sie folgende Schritte durch:
   - Klicken Sie auf der Registerkarte "Mitglied von" auf "Rolle hinzufügen".
   - Klicken Sie im Dialogfeld "Rolle(n) auswählen" auf "Symantec-Mitarbeiter Stufe 1" oder eine andere Rolle, der Sie diesen Benutzer zuweisen möchten, und klicken Sie dann auf "OK".
     Wenn keine der vordefinierten Sicherheitsrollen Ihre Anforderungen erfüllt, können Sie eine benutzerdefinierte Sicherheitsrolle erstellen.
     Siehe "Erstellen und Konfigurieren von Sicherheitsrollen" auf Seite 91.
4. Klicken Sie auf "Änderungen speichern".

Ermöglichen, dass Nicht-Administratorrollen Netzwerkerkennungsaufgaben erstellen oder ausführen können

Sie können Network Discovery-Aufgaben Benutzern außerhalb der Gruppe "Symantec Administratoren" zuweisen. Zum Delegieren von Aufgaben weisen Sie Privilegien an Nicht-Administrator-Rollen zu. Sie fügen dann diesen Nicht-Administrator-Rollen Benutzer hinzu.

Dieses Thema beschreibt das Delegieren häufiger Netzwerkerkennungsaufgaben an folgende Nicht-Administratorrollen:

- Symantec-Vorgesetzte
  Standardmäßig können Benutzer in dieser Rolle vorhandene Network Discovery-Aufgaben ausführen. Jedoch können sie Aufgaben nicht standardmäßig erstellen. Das liegt daran, dass sie keinen Zugriff auf das Standardverbindungsprofil haben, es sei denn, Sie gewähren diesen Zugriff ausdrücklich.
- Symantec Mitarbeiter Stufe 1 und Symantec Mitarbeiter Stufe 2
  Benutzer in diesen Rollen haben begrenzte Rechte. Sie können nicht mal vorhandene Aufgaben ausführen, bis Sie ihnen das Recht dazu erteilen.

Sie sind nicht auf die Nutzung dieser Nicht-Administrator-Rollen beschränkt. Sie werden in diesem Thema als Beispiele gezeigt. Verwenden Sie eine beliebige vordefinierte Sicherheitsrolle, die Ihrem Zweck dient.

Siehe "Vordefinierte Sicherheitsrollen" auf Seite 112.

Aufgaben verwenden Verbindungsprofile, die Identifikationsdaten verwenden. Damit jede Nicht-Administrator-Rolle neue Aufgaben erstellen (und nicht nur ausführen) kann, müssen Sie Zugriffsberechtigungen für Verbindungsprofile festlegen. Anschließend legen Sie eine Kontrollstufe (die maximale Stufe ist Vollständige Kontrolle) für die Protokolleinstellungen dieser Rolle fest. Nachdem Sie diese Berechtigungen festgelegt haben, können Benutzer mit der Nicht-Administrator-Rolle die von Ihnen angegebenen Aufgaben durchführen.

Damit Nicht-Administratoren Netzwerkerkennungsaufgaben erstellen können, müssen Sie die folgenden Verfahren abschließen:

- Gewähren Sie einer Nicht-Administratorrolle Rechte für das Aufgabenmanagement der Netzwerkerkennung. Mit diesem Verfahren können Benutzer mit dieser Rolle Aufgaben ausführen.
- Fügen Sie den Zugriffsberechtigungen des relevanten Verbindungsprofils die Rolle Ihrer Wahl hinzu. Ermöglichen Sie es dieser Rolle dann, Protokolleinstellungen zu steuern. Nachdem Sie die Rolle einem Verbindungsprofil hinzugefügt haben, können Benutzer in dieser Rolle Netzwerkerkennungsaufgaben erstellen und bearbeiten.

Diese Aufgabe ist ein Schritt im Prozess für die Delegierung von Netzwerkerkennungsaufgaben an Nicht-Administratoren.

Siehe "Delegieren von Netzwerkerkennungsaufgaben an Nicht-Administratorbenutzer" auf Seite 229.

So gewähren Sie einer Nicht-Administratorrolle Rechte für das Aufgabenmanagement der Netzwerkerkennung

1. Loggen Sie sich bei der Symantec Management-Plattform als Administrator ein.
2. Klicken Sie in der Symantec Management Console im Menü Einstellungen auf "Sicherheit > Kontoverwaltung".
3. Klicken Sie im linken Teilfenster unter "Kontoverwaltung" auf "Rollen".
4. Klicken Sie auf der Seite "Rollen" im linken Teilfenster auf die Nicht-Administratorrolle, an die Sie das Erstellen und Ausführen von Netzwerkerkennungsaufgaben delegieren möchten.

   Typische Rollen, an die Administratoren diese Aufgaben delegieren, sind "Symantec Mitarbeiter Stufe 1" und "Symantec Mitarbeiter Stufe 2".
5. Klicken Sie rechts in dem Fenster, das mit der von Ihnen ausgewählten Rolle bezeichnet ist, auf die Registerkarte "Privilegien", wenn sie nicht aktiv ist.
6. Aktivieren Sie unter "Managementprivilegien" die Option "Erkennungsaufgabenverwaltung".
7. Wenn die von Ihnen ausgewählte Rolle auch Verbindungsprofile erstellen oder bearbeiten muss, aktivieren Sie die folgenden zusätzlichen Optionen:
   - Aktivieren Sie unter "Verbindungsprofil-Privilegien" die Option "Verbindungsprofil erstellen".
   - Aktivieren Sie unter "Systemprivilegien" die Option "Sicherheit anzeigen".
   - Aktivieren Sie unter "Identifikationsdatenprivilegien" die Option "Identifikationsdaten erstellen".
8. Klicken Sie auf die Registerkarte Mitglieder.
9. Stellen Sie sicher, dass der Benutzer, den Sie der ausgewählten Rolle hinzufügen möchten, auch zu dieser Rolle hinzugefügt worden ist.

   Wenn der Benutzer kein Mitglied dieser Rolle ist, müssen Sie einen Notification Server-Benutzer erstellen und den Benutzer der relevanten Rolle hinzufügen.

   Siehe "Hinzufügen von Nicht-Administratorbenutzern zu den Sicherheitsrollen für die Ausführung von Netzwerkerkennungsaufgaben" auf Seite 233.
10. Klicken Sie auf Änderungen speichern.

So gewähren Sie einer vordefinierten Rolle vollständige (oder verringerte) Kontrolle über Protokolleinstellungen

1. Klicken Sie in der Symantec Management Console im Menü Einstellungen auf Alle Einstellungen.
2. Erweitern Sie im linken Teilfenster unter "Einstellungen" die Optionsfolge "Überwachung und Warnmeldungen > Protokollverwaltung > Verbindungsprofile" und klicken Sie auf "Verbindungsprofile verwalten".
3. Klicken Sie im Teilfenster "Verbindungsprofile verwalten" auf "Standardverbindungsprofil" und dann auf "Bearbeiten".
4. Klicken Sie im Dialogfeld Gruppeneinstellungen definieren auf Zugriffsberechtigungen für Protokolleinstellungen.
5. Klicken Sie auf Hinzufügen, wählen Sie die Rolle aus, der Sie die Kontrolle gewähren möchten, und klicken Sie auf Auswählen.

Symantec Mitarbeiter Stufe 1	Benutzer mit dieser Rolle haben standardmäßig weniger Rechte als "Symantec Vorgesetzte". Sobald Ihnen die Privilegien "Erkennungsaufgabenverwaltung" und "Vollständige Kontrolle" erteilt werden, können diese Mitarbeiter Network Discovery-Aufgaben erstellen und ausführen.
Symantec Mitarbeiter Stufe 2	Benutzer mit dieser Rolle haben standardmäßig weniger Rechte. Sobald Ihnen die Privilegien "Erkennungsaufgabenverwaltung" und "Vollständige Kontrolle" erteilt werden, können diese Mitarbeiter Network Discovery-Aufgaben erstellen und ausführen.
Symantec Vorgesetzte	Benutzer mit dieser Rolle können Network Discovery-Aufgaben standardmäßig ausführen. Sobald ihnen vollständige Kontrolle erteilt wird, können diese Mitarbeiter auch Network Discovery-Aufgaben erstellen und bearbeiten.

6. Wählen Sie im Dialogfeld "Berechtigungsauswahl" Berechtigungen mit einer der folgenden Methoden:
   - Aktivieren Sie "Verwenden" und "Lesen". Sie können alle anderen Felder aktivieren, die den Aufgaben entsprechen, zu deren Ausführung die ausgewählte Rolle berechtigt sein soll. Klicken Sie dann auf "Auswählen".
   - Klicken Sie auf "Vollständige Kontrolle", um der Rolle alle verfügbaren Rechte zu geben, die aufgelistet werden, und dann auf "Auswählen".

7 Klicken Sie im Dialogfeld Sicherheitsdeskriptor-Einstellungen für: Standardverbindungsprofil auf Übernehmen.

8 Klicken Sie im Dialogfeld Gruppeneinstellungen definieren auf OK, um das Verbindungsprofil zu speichern.

Gewähren von Privilegien zur Erstellung von Identifikationsdaten und Verbindungsprofilen für Nicht-Administratorrollen

Wenn Sie Aufgaben an Nicht-Administrator-Rollen delegieren, müssen Sie festlegen, welche Aufgaben die Benutzer, denen diese Rollen zugewiesen wurden, durchführen können. Jede vordefinierte Sicherheitsrolle in der Symantec Management-Plattform enthält dazu gehörende Rechte.

Siehe "Vordefinierte Sicherheitsrollen" auf Seite 112.

Beispiel: Die Standardrolle "Symantec Vorgesetzte" Benutzer, die dieser Rolle zugewiesen wurden, können bestehende Aufgaben ausführen, ohne dass der Rolle zusätzliche Privilegien gewährt werden. Diese Benutzer können auch Network Discovery-Aufgaben erstellen, wenn sie Zugriff auf ein vorhandenes Verbindungsprofil haben.

Um jedoch Nicht-Administrator-Rollen neue Aufgaben und Verbindungsprofile erstellen zu lassen, erteilen Sie jenen Rollen Rechte, um Identifikationsdaten und Verbindungsprofile zu erstellen. Diese zusätzlichen Rechte sind notwendig, wenn Benutzer neue Aufgaben erstellen sollen, die möglicherweise einige Identifikationsdaten und Verbindungsprofile erfordern, die sich von den vorhandenen Identifikationsdaten und Profilen unterscheiden.

Siehe "Konfigurieren von Erkennungseinstellungen" auf Seite 218.

Sie müssen diese Privilegien für die Rolle ermöglichen, um Nicht-Administrator-Rollen zugewiesene Benutzer Identifikationsdaten und Verbindungsprofile erstellen zu lassen. Mit diesen Rechten können die Benutzer diejenigen Identifikationsdaten und Verbindungsprofile erstellen, die für die Aufgaben geeignet sind, die Sie ihnen zugewiesen haben oder die sie erstellen.

Diese Aufgabe ist ein Schritt im Prozess für die Delegierung von Network Discovery-Aufgaben an Nicht-Administratoren.

Siehe "Delegieren von Netzwerkerkennungsaufgaben an Nicht-Administratorbenutzer" auf Seite 229.

So gewähren Sie Nicht-Administrator-Rollen Privilegien zur Erstellung von Identifikationsdaten und Verbindungsprofilen

1. Loggen Sie sich bei der Symantec Management Console als Administrator ein.
2. Klicken Sie in der Symantec Management Console im Menü Einstellungen auf Sicherheit > Kontoverwaltung.
3. Klicken Sie unter Kontoverwaltung auf Rollen
4. Klicken Sie im Teilfenster "Rollen" auf die Rolle, die Sie aktivieren möchten, und klicken Sie anschließend im rechten Teilfenster auf die Registerkarte "Privilegien".
5. Führen Sie einen Bildlauf zu Verbindungsprofil-Privilegien durch und aktivieren Sie Verbindungsprofil erstellen.
6. Führen Sie einen Bildlauf zu Identifikationsdatenprivilegien durch und aktivieren Sie Identifikationsdaten erstellen.
7. Scrollen Sie zu "Systemprivilegien" und aktivieren Sie die Option "Sicherheit anzeigen".
8. Klicken Sie auf "Änderungen speichern".

Erteilen von Zugriff für Nicht-Administrator-Rollen auf das Standardverbindungsprofil

Benutzer in Nicht-Administrator-Rollen benötigen Zugriff auf das Standardverbindungsprofil, um Aufgaben auszuführen. Nachdem Sie diesen Rollen Zugriff auf das Standardverbindungsprofil erteilt haben, können Benutzer in diesen Rollen auch Aufgaben erstellen. Sie können keine Verbindungsprofile erstellen, aber sie können Aufgaben erstellen, die vorhandene Verbindungsprofile verwenden.

Diese Aufgabe ist ein Schritt im Prozess für die Delegierung von Network Discovery-Aufgaben an Nicht-Administratoren.

Siehe "Delegieren von Netzwerkerkennungsaufgaben an Nicht-Administratorbenutzer" auf Seite 229.

So erteilen Sie einer vordefinierten Rolle volle (oder geringe) Kontrolle über das Standardverbindungsprofil

1. Klicken Sie in Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster unter Einstellungen die Optionsfolge Überwachung und Warnmeldungen > Protokollverwaltung > Verbindungsprofile und klicken Sie auf Verbindungsprofile verwalten.

3. Klicken Sie im Teilfenster "Verbindungsprofile verwalten" auf "Standardverbindungsprofil" und dann auf "Bearbeiten".
4. Klicken Sie im Dialogfeld "Gruppeneinstellungen definieren" auf "Zugriffsberechtigungen für Protokolleinstellungen".

Aktivieren der Erstellung und Ausführung von Aufgaben durch andere Rollen als die vordefinierten Sicherheitsrollen mithilfe des Network Discovery-Assistenten

Der Network Discovery-Assistent ist ein Administratortool, das zusammen mit der Symantec Management-Plattform erhältlich ist. Es ist eine Methode zur Erkennung von Netzwerkgeräten und zur Durchführung anderer Erkennungsaufgaben.

Sie rufen den Network Discovery-Assistenten im Menü Startseite der Symantec Management Console auf.

Siehe "Erstellen von "Network Discovery"-Aufgaben mithilfe des Assistenten" auf Seite 220.

Die folgenden Sicherheitsrollen sind vordefiniert und können standardmäßig Aufgaben unter Verwendung des Network Discovery-Assistenten erstellen und ausführen:

- Administrator
- Symantec-Supervisor
- Symantec Mitarbeiter Stufe 2
- Symantec Mitarbeiter Stufe 1

Eventuell möchten Sie andere Rollen aktivieren, um Aufgaben mit dem Network Discovery-Assistenten zu erstellen und auszuführen. In diesem Fall müssen Sie diesen Rollen die Rechte gewähren, die zur Durchführung dieser Aufgaben unter Verwendung des Assistenten erforderlich sind.

Diese Aufgabe ist ein Schritt im Prozess für die Delegierung von Network Discovery-Aufgaben an Nicht-Administratoren.

Siehe "Delegieren von Netzwerkerkennungsaufgaben an Nicht-Administratorbenutzer" auf Seite 229.

So aktivieren Sie andere Rollen als vordefinierte Sicherheitsrollen, um Aufgaben unter Verwendung des Network Discovery-Assistenten zu erstellen

1. Loggen Sie sich bei der Symantec Management-Plattform als Administrator ein.
2. Klicken Sie in der Symantec Management Console im Menü Einstellungen auf Sicherheit > Berechtigungen.
3. Klicken Sie unter "Sicherheitsrollenmanager" im Dropdown-Feld "Rolle" auf die Rolle, die Sie zur Ausführung von Aufgaben berechtigen möchten.
4. Klicken Sie in der Dropdown-Liste "Ansicht" auf "Einstellungen".
5. Klicken Sie im linken Teilfenster auf "Bearbeiten".

   Beachten Sie, dass im Dialogfeld Elementauswahl alle weiteren Optionen grau dargestellt sind, wenn das Kontrollkästchen Einstellungen aktiviert ist.
6. Wenn das Kontrollkästchen Einstellungen aktiviert ist, deaktivieren Sie es.
7. Aktivieren Sie unter "Erkennung und Inventarisierung" die Option "Network Discovery-Assistent", wenn sie nicht bereits aktiviert ist.
8. Aktivieren Sie die Option Einstellungen erneut, um die Vererbung wieder einzuschalten.
9. Klicken Sie auf Änderungen speichern.

So aktivieren Sie andere Rollen als vordefinierte Sicherheitsrollen, um Aufgaben unter Verwendung des Network Discovery-Assistenten zu planen und auszuführen

1. Loggen Sie sich bei der Symantec Management-Plattform als Administrator ein.
2. Klicken Sie in der Symantec Management Console im Menü Einstellungen auf Sicherheit > Berechtigungen.
3. Klicken Sie unter Sicherheitsrollenmanager im Dropdown-Feld Rolle auf die Rolle, die Sie aktivieren möchten.
4. Klicken Sie im Dropdown-Feld Ansicht auf Aufgaben.
5. Erweitern Sie im linken Teilfenster unter Aufgaben die Optionsfolge Jobs und Aufgaben > Systemjobs und -aufgaben und klicken Sie auf Erkennung und Inventarisierung.

   Beachten Sie, dass im Teilfenster Erkennung und Inventarisierung der Abschnitt Geerbt grau dargestellt ist und nicht bearbeitet werden kann.

6 Scrollen Sie im Teilfenster "Erkennung und Inventarisierung" im Abschnitt "Nicht geerbt" nach unten zu "Task Server-Berechtigungen" und aktivieren Sie die Option "Aufgabe ausführen".

7 Klicken Sie auf "Änderungen speichern" und schließen Sie den "Sicherheitsrollenmanager".

Aktivieren des Schreibschutzes für ein Verbindungsprofil

Sie müssen möglicherweise Network Discovery-Aufgaben an Benutzer mit Nicht-Administrator-Rollen delegieren. Jedoch möchten Sie unter Umständen nicht, dass diese Benutzer Verbindungsprofile ändern. Machen Sie ein Verbindungsprofil schreibgeschützt, um Hackerversuche zu verhindern und die Sicherheit und den Datenschutz von vertraulichen Informationen aufrecht zu erhalten. Ein weiterer Grund rür ein schreibgeschütztes Verbindungsprofil ist, dass verhindert werden kann, dass weniger erfahrene Benutzer ein Verbindungsprofil ändern, um nicht unterstützte Protokolle zu verwenden.

Wenn Sie Benutzer auf das Anzeigen von Identifikationsdaten und das Ausführen von Network Discovery-Aufgaben beschränken möchten, können Sie Schreibrechte für jedes Verbindungsprofil blockieren. Indem Sie die Schreibrechte einer Nicht-Administrator-Rolle blockieren, machen Sie ein Verbindungsprofil für Benutzer mit dieser Rolle schreibgeschützt. Die Benutzer, die diesen Nicht-Administratorrollen zugewiesen sind, deren Schreibrechte Sie blockieren, können immer noch Aufgaben ansehen und ausführen, aber sie können dieses Verbindungsprofil nicht ändern oder ein Verbindungsprofil erstellen.

Diese Aufgabe ist ein Schritt im Prozess für die Delegierung von Network Discovery-Aufgaben an Nicht-Administratoren.

Siehe "Delegieren von Netzwerkerkennungsaufgaben an Nicht-Administratorbenutzer" auf Seite 229.

So aktivieren Sie den Schreibschutz für ein Profil

1 Loggen Sie sich bei der Symantec Management Console als Administrator ein.

2 Klicken Sie in der Symantec Management Console im Menü Einstellungen auf Alle Einstellungen.

3 Erweitern Sie im linken Teilfenster unter Einstellungen die Optionsfolge Überwachung und Warnmeldungen > Protokollverwaltung > Verbindungsprofile und klicken Sie auf Verbindungsprofile verwalten.

4 Klicken Sie im Teilfenster "Verbindungsprofile verwalten" auf "Standardverbindungsprofil" und dann auf "Bearbeiten".

5 Klicken Sie im Dialogfeld Gruppeneinstellungen definieren auf Zugriffsberechtigungen für Protokolleinstellungen.

6 Wählen Sie im Dialogfeld Sicherheitsdeskriptor-Einstellungen für: Standardverbindungsprofil die Rolle aus, wie zum Beispiel Symantec Mitarbeiter Stufe2, und klicken Sie auf Bearbeiten.

7 Deaktivieren Sie im Dialogfeld Berechtigungsauswahl die Option Schreiben und klicken Sie auf Auswählen.

8 Klicken Sie im Dialogfeld Sicherheitsdeskriptor-Einstellungen für: Standardverbindungsprofil auf Übernehmen, um die Einstellungen zu speichern, und im Dialogfeld Gruppeneinstellungen definieren auf OK, um das Verbindungsprofil zu speichern.

Importieren von MIB-Dateien

Sie können zwei Methoden verwenden, um MIB-Dateien in die Datenbank zu importieren. Sie können MIB-Dateien nacheinander unter Verwendung des Dienstprogramms für den MIB-Import manuell importieren. Sie können auch eine Aufgabe erstellen und planen, die eine oder mehrere MIB-Dateien importiert.

So importieren Sie MIB-Dateien unter Verwendung des Dienstprogramms für den MIB Import manuell

1 Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Alle Einstellungen".

2 Erweitern Sie im linken Teilfenster "Überwachung und Warnmeldungen > SNMP MIB-Import-Browser" und klicken Sie auf "MIB-Browser".

3 Klicken Sie auf der Seite "MIB-Browser" auf "MIB-Datei importieren".

4 Klicken Sie im Dialogfeld "MIB-Datei importieren" auf "Durchsuchen", wählen Sie die Datei aus und klicken Sie dann auf "Importieren".

Sie können zusätzliche MIB-Dateien importieren, die Sie benötigen.

So importieren Sie MIB-Dateien unter Verwendung der Aufgabe "MIB-Import"

1 Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Aufträge und Aufgaben".

2 Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, in dem die Aufgabe erstellt werden soll, und wählen Sie im Kontextmenü die Option "Neu > Aufgabe".

3 Klicken Sie im Dialogfeld "Neue Aufgabe erstellen" im linken Teilfenster unter "Überwachung und Warnmeldungen" auf "MIB-Import".

4 Benennen Sie die Aufgabe um, wählen Sie die hochzuladene MIB-Datei aus und geben Sie die Importoptionen an.

   Sie können entweder die einzelne MIB-Datei oder zusätzliche MIB-Dateien importieren, die im Verzeichnis gespeichert sind.

5 Klicken Sie auf "Upload, um die MIB-Datei in die Importaufgabe hochzuladen.

6 Wenn Sie mehrere MIB-Dateien importieren möchten, wählen Sie diese nacheinander aus und laden Sie sie einzeln hoch.

7 Klicken Sie auf "OK".

8 Wählen Sie die neue MIB-Importaufgabe aus.

   Standardmäßig wird die neue MIB-Import-Aufgabe hier gespeichert: "Systemaufträge und -aufgaben > Notification Server".

9 Planen Sie die Ausführung der neuen MIB-Importaufgabe unter Verwendung des Dienstprogramms für die Aufgabenplanung.

   Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.

Abschnitt 4

Installieren und Konfigurieren des Symantec Management-Agent

- Kapitel 14. Einführung in den Symantec Management-Agent
- Kapitel 15. Installieren des Symantec Management Agent auf Clientcomputern
- Kapitel 16. Aktualisieren und Deinstallieren des Symantec Management Agent
- Kapitel 17. Konfigurieren des Symantec Management Agent

Kapitel 14

Einführung in den Symantec Management-Agent

In diesem Kapitel werden folgende Themen behandelt:

- Infos zu Symantec Management-Agent
- Info zu Agent-Registrierung

Infos zu Symantec Management-Agent

Der Symantec Management-Agent stellt die Kommunikation zwischen dem Notification Server und den Computern im Netzwerk her. Computer, auf denen der Symantec Management-Agent installiert ist, werden "verwaltete Computer" genannt. Notification Server überwacht und verwaltet mithilfe des Symantec Management Agent die einzelnen Computer über Symantec Management Console.

Notification Server und Symantec Management Agent arbeiten zusammen, um die folgenden Funktionstypen für verwaltete Computer zur Verfügung zu stellen:

- Überwachung von Hardware und Software
- Planung von Softwareinstallationen und Datei-Updates
- Erfassung von Grundinventardaten
- Verwaltung von Richtlinien und Paketen

Sie können den Symantec Management-Agent auf Windows-, Linux-, UNIX- und Mac-Computern installieren. Mit Symantec Management-Agent können Sie auch Solution Agent-Plugins installieren und verwalten, durch die der Funktionsumfang des Agent erweitert wird. Durch die Installation des Inventory-Plugins können Sie

beispielsweise ausführliche Hardware- und Softwareinformationen von allen verwalteten Computern erfassen.

Siehe "Methoden für das Installieren des Symantec Management-Agent" auf Seite 248.

Wenn Sie die Cloud-fähige Verwaltung verwenden möchten, müssen Sie Symantec Management-Agent für diese Umgebung entsprechende installieren und einrichten.

Siehe "Info zu Cloud-fähiger Verwaltung" auf Seite 297.

Info zu Agent-Registrierung

Zusammen mit der Funktion für Cloud-fähige Verwaltung, mit der Sie Geräte außerhalb der Firewall verwalten können, wurde die Funktion für Agent-Registrierung zur IT Management Suite 7.5 hinzugefügt, um sicherzustellen, dass nur vertrauenswürdige Clientcomputer mit dem Notification Server kommunizieren können.

Siehe "Info zu Cloud-fähiger Verwaltung" auf Seite 297.

Bei der Funktion für Agent-Registrierung ist erforderlich, dass ein Clientcomputer für die Kommunikation mit dem Notification Server zugelassen ist, bevor er von diesem Notification Server verwaltet werden kann. Die Standardrichtlinie für Agent-Registrierung ermöglicht allen Computern eine Kommunikation mit dem Notification Server. Sie können jedoch auch benutzerdefinierte Richtlinien für die Agent-Registrierung erstellen, durch die bestimmte Computer zugelassen oder blockiert werden können.

Siehe "Erstellen einer Agent-Registrierungsrichtlinie" auf Seite 253.

Nachdem durch die Richtlinie für Agent-Registrierung ein Computer zugelassen oder blockiert wurde, können Sie anschließend den Status nur manuell auf der Berichtsseite "Agent-Registrierungsstatus" ändern. Beispielsweise können Sie Computer, die im ausstehenden Status sind, zulassen oder blockieren. Außerdem können Sie die Registrierung der Agents, die Sie zuvor zugelassen haben, widerrufen.

Siehe "Anzeigen und Verwalten des Agent-Registrierungsstatus" auf Seite 261.

Agent-Registrierung wird auf Windows-, UNIX-, Linux- und Mac-Plattformen unterstützt.

Kapitel 15

Installieren des Symantec Management Agent auf Clientcomputern

In diesem Kapitel werden folgende Themen behandelt:

- Methoden für das Installieren des Symantec Management-Agent
- Installieren des Symantec Management-Agent unter Windows
- Manuelle Installation von Symantec Management Agent auf UNIX-, Linux- und Mac-Computern

Methoden für das Installieren des Symantec Management-Agent

Bevor Sie den Symantec Management-Agent installieren, empfehlen wir, Ihre Installation unter Verwendung des *Planungs- und Implementierungshandbuchs für IT Management Suite* zu planen.

Sie können den Symantec Management-Agent unter Windows, UNIX oder MacOS installieren.

Siehe "Infos zu Symantec Management-Agent" auf Seite 246.

Nachdem der Symantec Management-Agent auf dem Clientcomputer installiert wurde, sendet er eine Registrierungsanfrage an den Notification Server, um eine vertrauenswürdige Kommunikation herzustellen.

Siehe "Info zu Agent-Registrierung" auf Seite 247.

Wenn Sie die Cloud-fähige Verwaltung verwenden möchten, müssen Sie Symantec Management-Agent für diese Umgebung entsprechende installieren und einrichten.

Siehe "Info zu Cloud-fähiger Verwaltung" auf Seite 297.

Tabelle 15-1 Methoden für das Installieren des Symantec Management-Agent

Methode	Beschreibung
Manuelle Push-Installation	Push-Installationen werden von der Symantec Management Console aus eingeleitet und installieren den Symantec Management-Agent sofort. Sie können den Symantec Management-Agent in einem einzigen Push-Vorgang auf einer beliebigen Anzahl von Computern installieren. Außerdem können Sie die Installationsoptionen für die jeweilige Push-Installation anpassen. Unter UNIX, Linux und MacOS erfordert diese Methode einen aktiven SSH-Server. Außerdem müssen Sie die Firewall so konfigurieren, dass SSH-Verbindungen auf den Zielcomputern akzeptiert werden. Siehe "Installieren des Symantec Management-Agent für Windows mit einer manuellen Push-Installation" auf Seite 256. Siehe "Installieren von Symantec Management-Agent für UNIX Linux und Mac mit einer manuellen Push-Installation" auf Seite 272. Agents, die mit einer manuellen Push-Installation installiert werden, umgehen die Agent-Registrierung und die Kommunikation zwischen dem Agent und dem Notification Server wird automatisch hergestellt.
Manuelle Pull-Installation	Die Pull-Installation wird von dem Computer aus eingeleitet, auf dem der Symantec Management-Agent installiert werden soll. Mit diesem Vorgang können Sie Firewalls und Netzwerk-Zugriffsbegrenzungen umgehen, die Push-Installationen auf Remote-Computern unter Umständen verhindern. Für UNIX-, Linux- und Mac-Computer müssen Sie diese Methode verwenden, wenn SSH nicht verfügbar ist. Siehe "Installieren des Symantec Management-Agent für Windows mit einer manuellen Pull-Installation" auf Seite 258. Siehe "Installieren von Symantec Management-Agent unter UNIX, Linux und Mac OS mit einer manuellen Pull-Installation" auf Seite 276.

Methode	Beschreibung
Geplante Push-Installation	Diese Methode ist für nur Windows-Computer verfügbar. Eine geplante Symantec Management-Agent-Installation wird zu einem festgelegten Zeitpunkt durchgeführt, im Gegensatz zu manuellen Push-Installationen, die sofort ausgeführt werden. Sie können den Symantec Management-Agent per Push-Installation auf Computern in einer Organisationsgruppe, einem Filter oder Ressourcenziel oder auf Computern mit ausgewählten Ressourcen installieren. Beachten Sie, dass die Agents, die Sie mit geplanter Push-Installation installieren, die Agent-Registrierung nicht umgehen. Siehe "Ausführen einer geplanten Installation des Symantec Management-Agent für Windows" auf Seite 259.
Agent-Upgrade-Richtlinie	Die Richtlinie "Symantec Management-Agent-Upgrade" ist im Lieferumfang der Symantec Management-Plattform enthalten. Sie können diese Richtlinie aktivieren und so konfigurieren, dass auf allen verwalteten Computern die richtige Version des Symantec Management-Agent installiert wird. Siehe "Konfigurieren von Aktualisierungs- und Deinstallationsrichtlinien für den Symantec Management-Agent" auf Seite 280.

Hinweis: Wenn Sie den Symantec Management-Agent auf einem Computer installieren, gibt es eine Verzögerung, bevor der Client Task Agent auf dem Notification Server registriert wird. Alle Aufgaben, die während dieser Zeit (gewöhnlich ca. 10 Minuten) diesen Computer als Ziel haben, werden in die Warteschlange gestellt, bis der Client Task Agent registriert wurde. Nachdem der Client Task Agent registriert wurde, werden die Aufgaben sofort ausgeführt.

Installieren des Symantec Management-Agent unter Windows

Sie können den Symantec Management-Agent mit einer manuellen Push- oder Pull-Installation installieren. Er wird empfohlen, den Symantec Management-Agent über eine manuelle Push-Installation auf ausgewählten Computern zu installieren. Befindet sich der Remote-Computer hinter einer Firewall oder hat er nur begrenzten Netzwerkzugriff, müssen Sie möglicherweise eine manuelle Pull-Installation ausführen.

Siehe "Infos zu Symantec Management-Agent" auf Seite 246.

Tabelle 15-2 Installieren des Symantec Management-Agent unter Windows

Schritt	Aktion	Beschreibung
Schritt 1	Überprüfen Sie, dass die Computer die Installationsvoraussetzungen erfüllen.	Jeder Computer muss die Hardware- und Softwarevoraussetzungen erfüllen, bevor Sie den Symantec Management-Agent auf ihm installieren können. Siehe "Anforderungen für das Installieren des Symantec Management-Agent unter Windows" auf Seite 252.
Schritt 2	(Optional) Definieren Sie die Agentregistrierungsrichtlinien.	Nachdem Sie den Symantec Management-Agent installiert haben, sendet er eine Registrierungsanforderung an den Notification Server, um ein Vertrauensverhältnis zwischen dem Server und dem Client aufzubauen. Die standardmäßige Agent-Registrierungsrichtlinie lässt die automatische Registrierung aller Agents zu. Sie können die Standardrichtlinie ändern oder benutzerdefinierte Richtlinien erstellen, um Regeln mit Einschränkungen anzugeben. Siehe "Erstellen einer Agent-Registrierungsrichtlinie" auf Seite 253.
Schritt 3	Geben Sie die Installationseinstellungen an.	Bevor Sie die manuelle Push- bzw. Pull-Installation des Symantec Management-Agent durchführen, müssen Sie die Installationseinstellungen angeben. Siehe "Angeben des Symantec Management-Agent für Windows-Installationseinstellungen" auf Seite 256.
Schritt 4	Installieren Sie den Symantec Management-Agent mit dem geeigneten Verfahren.	Das bevorzugte Verfahren ist eine Push-Installation von Symantec Management-Agent auf den ausgewählten Computern. Wenn sich ein Computer jedoch hinter einer Firewall befindet oder schwer für den Notification Server zu erreichen ist, können Sie stattdessen eine Pull-Installation des Symantec Management-Agent durchführen. Siehe "Installieren des Symantec Management-Agent für Windows mit einer manuellen Push-Installation" auf Seite 256. Siehe "Installieren des Symantec Management-Agent für Windows mit einer manuellen Pull-Installation" auf Seite 258. Siehe "Ausführen einer geplanten Installation des Symantec Management-Agent für Windows" auf Seite 259.

Schritt	Aktion	Beschreibung
Schritt 5	Anzeigen des Installationsstatusberichts, um erfolgreiche Installation zu überprüfen.	Der Installationsstatusbericht enthält die Details aller manuellen Push-Installationen sowie geplante Symantec Management-Agent-Installationen, die versucht worden sind. Der Bericht umfasst nicht die Details von Pull-Installationen. Siehe "Anzeigen des Installationsstatusberichts" auf Seite 260.
Schritt 6	Zeigen Sie den Agent-Registrierungsstatus an und verwalten Sie ihn, um die erfolgreiche Registrierung zu prüfen.	Mit dem Bericht "Agent-Registrierungsstatus" können Sie alle Registrierungsanforderungen und abgeschlossenen Registrierungen von Symantec Management-Agents anzeigen und verwalten. Siehe "Anzeigen und Verwalten des Agent-Registrierungsstatus" auf Seite 261.

Anforderungen für das Installieren des Symantec Management-Agent unter Windows

Bevor Sie den Symantec Management-Agent installieren können, müssen Sie die Computer konfigurieren und prüfen, ob sie den Installationsanforderungen entsprechen.

Siehe "Methoden für das Installieren des Symantec Management-Agent" auf Seite 248.

Diese Aufgabe ist ein Schritt beim manuellen Installieren des Symantec Management-Agent unter Windows.

Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.

Tabelle 15-3 Anforderungen für die Installation des Symantec Management-Agent unter Windows

Anforderung	Beschreibung
Betriebssystem	Folgende Betriebssysteme werden unterstützt: ■ Windows Server 2003 SP2 (x86, x64) ■ Windows Server 2003 R2 und höher (x86, x64) ■ Windows XP Professional SP2 (x64) ■ Windows XP Professional SP3 (x86) ■ Windows Vista SP2 und höher (x86, x64) ■ Windows Server 2008 und höher (x86, x64) ■ Windows Server 2008 R2 und höher (x86, x64) ■ Windows 7 und höher (x86, x64)

Anforderung	Beschreibung
Festplattenspeicher	60 MB
RAM	64 MB (128 MB empfohlen)
Internet Explorer	Version 6.0 oder höher
Zugriffsrechte	Lokale Administratorrechte
Firewall	Der Computer muss in der Lage sein, mit Symantec Management-Plattform durch die Firewall des Computers zu kommunizieren. Führen Sie einen der folgenden Schritte aus: ■ Aktivieren Sie in den Firewall-Einstellungen die Option "Datei- und Druckerfreigabe". ■ Fügen Sie Port UDP 138, TCP 445, TCP 80 (oder TCP 443 für HTTPS) und ICMP-Typ 8 als eingehende Portausnahmen hinzu. Sie können die Ports mithilfe einer Gruppenrichtlinie hinzufügen. ■ Deaktivieren Sie die Firewall.
Einfache Dateifreigabe (Windows XP nur in Nicht-Domänenumgebungen)	Für Clientcomputer mit Windows XP in Nicht-Domänenumgebungen, müssen Sie außerdem in Windows XP unter "Ordneroptionen" die Option "Einfache Dateifreigabe verwenden" deaktivieren.
Benutzer-Zugriffssteuerung (Windows Vista und Windows 7 nur Nicht-Domänenumgebungen)	Für Clientcomputer mit Windows Vista oder 7 in Nicht-Domänenumgebungen, müssen Sie außerdem die Benutzer-Zugriffssteuerung deaktivieren.

Erstellen einer Agent-Registrierungsrichtlinie

Mithilfe von Agent-Registrierungsrichtlinien können Sie den Agent-Registrierungsvorgang automatisieren. Eine Agent-Registrierungsrichtlinie besteht aus mehreren Regeln, die festlegen, wie die eingehenden Registrierungsanforderungen verarbeitet werden. Im Inhalt der Registrierungsanforderung sendet der Symantec Management-Agent seinen Hostnamen, seine MAC-Adresse, IP-Adresse, FQDN und eingeloggte Benutzerdaten. Die Agent-Registrierungsrichtlinie verwendet die Registrierungsanforderungsdaten sowie die von Ihnen im Rahmen der Richtlinie definierten Regeln, wonach entschieden wird, ob die Anforderung zugelassen oder blockiert wird.

Warnung: Die Agent-Standardregistrierungsrichtlinie lässt automatisch zu, dass alle Agents mit Notification Server kommunizieren. Sie können die Standardrichtlinie ändern oder benutzerdefinierte Richtlinien erstellen, um die Agents einzuschränken, die mit Notification Server kommunizieren können. Wenn keine aktiven Richtlinien verfügbar sind, wird der Status jeder eingehenden Registrierungsanforderung auf "Ausstehend" eingestellt.

Sie können die Registrierunganforderungen im Bericht "Agent-Registrierungsstatus" anzeigen. Sie können in der Symantec Management Console unter "Berichte > Notification Server Management > Registrierung" auf diesen Bericht zugreifen.

Siehe "Anzeigen und Verwalten des Agent-Registrierungsstatus" auf Seite 261.

Diese Aufgabe ist ein optionaler Schritt in den folgenden Prozessen:

- Installieren des Symantec Management-Agent auf Windows-Computern.
  Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.
- Manuelles Installieren des Symantec Management-Agent auf UNIX-, Linux- und Mac-Computern.
  Siehe "Manuelle Installation von Symantec Management Agent auf UNIX-, Linux- und Mac-Computern" auf Seite 266.

So erstellen Sie eine Agent-Registrierungsrichtlinie

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster unter "Einstellungen" die Optionsfolge "Agents/Plugins > Symantec Management-Agent > Einstellungen".
3. Klicken Sie mit der rechten Maustaste auf "Registrierungsrichtlinien" und wählen Sie "Neu > Registrierungsrichtlinie".
4. Legen Sie im rechten Teilfenster die Einstellungen der Agent-Registrierungsrichtlinie wie folgt fest:

Regeln	Mit dieser Option können Sie verschiedene Typen von Masken zur Agent-Erkennung mithilfe der Anforderungsdaten definieren. Beispielsweise können Sie Masken für einen Hostnamen, eine IP-Adresse und einen eingeloggten Benutzernamen definieren. Eine einzelne Richtlinie kann eine unbegrenzte Anzahl von Masken jedes Typs enthalten. Während des Maskenübereinstimmungsprozesses behandelt Notification Server verschiedene Maskentypen als logische AND-Operation und ähnliche Maskentypen als logische OR-Operation. Beispiel: Eine Richtlinie mit den folgenden Masken ermöglicht die Registrierung aller Agents mit dem Namen, der mit der Maske "*test" übereinstimmt, und ihre IP-Adresse ist entweder 10.31.12.1, 10.31.12.2 oder eine beliebige von 255 IP-Adressen aus dem 10.31.15.0-Subnetz: ■ Host = *test ■ IP=10.31.12.1 ■ IP=10.31.12.2 ■ IP=10.31.15.0/24 **Hinweis:** Sternchen wird für alle Regeln mit Ausnahme von IP-Adresse akzeptiert. Wenn Sie einen IP-Adressbereich in einer Regel angeben möchten, müssen Sie ihn mit der Subnetzmaske definieren. Beispiel: Anstatt **10.31.15.*** einzugeben, geben Sie **10.31.15.0/24** ein.
Aktionen	Mit dieser Option definieren Sie die Regel für die den Vorgaben entsprechende Agentverarbeitung mit den folgenden Optionen: ■ Zulassen Die Agents werden automatisch registriert und Sie müssen sie nicht manuell akzeptieren. ■ Blockieren Anforderungen von diesen Agents werden abgelehnt. Hinweis: Wenn zwei Richtlinien auf eine Registrierunganforderung anwendbar sind und eine von ihnen die Registrierung zulässt, während die andere sie blockiert, wird die blockierende Richtlinie auf die Anforderung angewendet.

5 Aktivieren Sie die Richtlinie.

Klicken Sie oben rechts auf der Seite auf den farbigen Kreis und dann auf "Ein".

6 Klicken Sie auf "Änderungen speichern".

Angeben des Symantec Management-Agent für Windows-Installationseinstellungen

Mit den Installationseinstellungen geben Sie an, wie der Symantec Management-Agent auf dem Clientcomputer installiert werden soll. Sie können die Installationsoptionen auf eine manuelle Push- bzw. Pull-Installation des Symantec-Management Agent festlegen. Beachten Sie, dass Sie diese Einstellungen nicht in einer CSV-Datei einschließen können, wenn Sie Computernamen importieren.

Diese Aufgabe ist ein Schritt im Installationsprozess des Symantec Management-Agent auf Windows-Computern.

Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.

So legen Sie die Windows-Installationsoptionen für Symantec Management-Agent fest

1. Klicken Sie in der "Symantec Management Console" im Menü "Aktionen" auf "Agents/Plugins > Symantec Management-Agent".
2. Klicken Sie auf der Seite "Symantec Management-Agent – Installation" unter "Agent-Rollout an Computer" auf "Einstellungen".
3. Aktivieren Sie im Dialogfeld "Symantec Management-Agent – Installationsoptionen" die gewünschten Optionen und geben Sie die notwendigen Einstellungen in den entsprechenden Feldern an. Klicken Sie anschließend auf "OK".

   Für weitere Informationen klicken Sie auf die Seite und drücken Sie dann **"F1"**.
4. Klicken Sie auf der Seite "Symantec Management-Agent-Installation" auf "Änderungen speichern".

Installieren des Symantec Management-Agent für Windows mit einer manuellen Push-Installation

Sie können den Symantec Management-Agent auf einen beliebigen Windows-Computern per Push-Installation installieren. Bevor Sie den Symantec Management-Agent manuell auf der Seite "Symantec Management-Agent installieren" installieren oder deinstallieren können, müssen Sie die Zielcomputer auswählen. Sie können die Computernamen manuell eingeben, die mit der Ressourcenerkennung erkannten Computer auswählen, oder die Computer aus einer CSV-Datei importieren. Die CSV-Datei ist eine kommagetrennte Textdatei. Die Datei enthält die DNS-Namen oder die IP-Adressen der Clientcomputer, auf denen der Symantec Management-Agent installiert werden soll. Für Windows ist die CSV-Datei einfach eine Liste von Computernamen oder IP-Adressen, die auf

der Seite "Symantec Management-Agent installieren" importiert werden. Elemente werden als Namen von Computern oder IP-Adressen interpretiert (Einträge, die im entsprechenden Format vorliegen). Leerzeichen sind nicht zulässig: Element, die Leerzeichen enthalten, werden ignoriert.

Hinweis: Sie können den Symantec Management-Agent nur auf den Computern manuell installieren, die unter Verwendung der Domänen-Ressourcenerkennung oder der Network Discovery erkannt wurden.

Diese Aufgabe ist ein Schritt beim Installieren des Symantec Management-Agent unter Windows.

Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.

So installieren Sie den Symantec Management-Agent für Windows mit einer manuellen Push-Installation

1. Wählen Sie in der Symantec Management Console im Menü "Aktionen" die Option "Agents/Plugins > Symantec Management-Agent - Push".
2. Wählen Sie auf der Seite "Symantec Management-Agent installieren" auf der Registerkarte "Agent installieren" unter "Agent-Rollout an Computer" die Computer aus, auf denen Symantec Management-Agent installiert werden soll und klicken Sie auf "Installieren".

So fügen Sie einen Computer manuell hinzu	Geben Sie im Textfeld den Computernamen (muss ein auflösbarer DNS-Name sein) oder die IP-Adresse ein und klicken Sie dann auf "Hinzufügen".
So wählen Sie aus den verfügbaren Computern aus	1 Klicken Sie auf "Ausgewählte Computer". 2 Fügen Sie im Dialogfeld "Computer auswählen" die gewünschten Computer aus der Liste "Verfügbare Computer" der Liste "Ausgewählte Computer" hinzu und klicken Sie dann auf "OK".

So importieren Sie Computer aus einer CSV-Datei

1. Klicken Sie in der Symbolleiste unter "Agent-Rollout an Computer" auf "Computer aus einer ausgewählten Datei importieren".
2. Wählen Sie im Dialogfeld "Zu importierende Datei auswählen" die gewünschte CSV-Datei aus und klicken Sie auf "Öffnen".

3. Konfigurieren Sie im Dialogfeld "Symantec Management-Agent - Installationsoptionen" die Installationseinstellungen, und klicken Sie dann auf "Installation fortsetzen".

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.

   Auf der Seite "Symantec Management Agent – Installation" unter "Agent-Rollout an Computer" zeigt die Spalte "Status" in der Computerliste an, ob die Installation auf jedem Computer erfolgreich ausgeführt wurde oder fehlgeschlagen ist. Beachten Sie, dass ein neu installierter Symantec Management-Agent seinen Status an den ursprünglichen Notification Server sendet, selbst wenn er von einem anderen Notification Server verwaltet wird.

Installieren des Symantec Management-Agent für Windows mit einer manuellen Pull-Installation

Wenn Sie den Symantec Management-Agent auf Remote-Computern installieren möchten, die begrenzten Netzwerkzugriff haben oder sich hinter einer Firewall befinden, müssen Sie möglicherweise eine Pull-Installation des Symantec Management-Agent auf jedem Computer ausführen. Sie können sich bei jedem Computer einloggen, auf Notification Server über eine URL zugreifen und die Installation des Symantec Management-Agent starten. Die Installation läuft dann automatisch, ohne weiteren Benutzereingriff.

Siehe "Infos zu Symantec Management-Agent" auf Seite 246.

Bei der Pull-Installation des Symantec Management-Agent werden die Einstellungen im Dialogfeld "Symantec Management-Agent – Installationsoptionen" verwendet, mit Ausnahme von "Agent-Paket vom nächsten Package Server herunterladen", da diese irrelevant ist.

Die URL der Seite "Symantec Management Agent-Download" wird auf der Seite "Symantec Management Agent-Installation" unter "URL der Download-Seite" angezeigt. Sie können diese Einstellung nicht ändern.

Diese Aufgabe ist ein Schritt beim Installieren des Symantec Management-Agent unter Windows.

Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.

So zeigen Sie die Seite zum Herunterladen des Symantec Management-Agent an

1. Klicken Sie in der Symantec Management Console im Menü "Aktionen" auf "Agents/Plugins" > "Symantec Management-Agent – Push".
2. Klicken Sie auf der Seite "Symantec Management Agent-Installation" unter "URL der Download-Seite" auf "Diese Seite anzeigen".

So installieren Sie den Symantec Management-Agent für Windows mit einer manuellen Pull-Installation

1. Melden Sie sich als Administrator am Computer an.

   Sie können sich remote mit Hilfe einer Remote-Zugriffsanwendung wie z.B. pcAnywhere einloggen oder Sie können einen Benutzer am Remote-Standort mit dem geeigneten Konto einloggen lassen.
2. Öffnen Sie auf dem Remote-Computer Internet Explorer und rufen folgende URL auf:

   http://*NSName*/Altiris/NS/Agent/AltirisAgentDownload.aspx

   wobei *NSName* der Name Ihres Notification Server-Computers ist.
3. Klicken Sie im Fenster "Symantec Management-Agent - Download" auf "Klicken Sie hier, um den Download und die Installation zu starten.".

   Die Installation des Agent läuft im Hintergrund und erfordert keine weitere Aktion.

Ausführen einer geplanten Installation des Symantec Management-Agent für Windows

Sie können eine geplante Installation des Symantec Management-Agent konfigurieren. Eine geplante Installation wird, anders als manuelle Push-Installationen, die sofort durchgeführt werden, zur angegebenen Zeit durchgeführt. Beispiel: Wenn Sie den Agent auf einer bestimmten Computergruppe zu einer bestimmten Zeit installieren möchten, können Sie einen Zeitplan ohne Wiederholung einrichten, der zur gegebenen Zeit ausgeführt wird.

Sie können auch einen Zeitplan konfigurieren, um den Symantec Management-Agent automatisch auf neuen Computern zu installieren, wenn sie der Umgebung hinzugefügt werden. Der Ressourcenerkennungszeitplan wird täglich ausgeführt, um neue Computer zu erkennen, und Sie können Filter konfigurieren, um die neuen Computer den passenden Gruppen zuzuweisen. Sie können die Symantec Management-Agent-Installation für alle Computer in bestimmten Gruppen in geeigneten Abständen planen.

Gehen Sie nicht unüberlegt an die Implementierung einer automatischen Installationsmethode heran. Wir empfehlen, dass Sie einen manuellen Schritt einschließen, um zu überprüfen, ob der Agent auf den Computern installiert wurde.

Diese Aufgabe ist ein Schritt beim Installieren des Symantec Management-Agent unter Windows.

Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.

So konfigurieren Sie einen Installationszeitplan für den Symantec Management-Agent unter Windows

1. Klicken Sie in der Symantec Management Console im Menü "Aktionen" auf "Agents/Plugins > Symantec Management-Agent - Push".
2. Klicken Sie rechts auf der Seite "Symantec Management Agent – Installation" unter "Geplante Push-Installation auf Computer" auf den farbigen Kreis und klicken Sie dann auf "Ein".
3. Geben Sie unter "Zuordnen zu" die Computer an, auf denen der Symantec Management-Agent installiert werden soll.

   Sie können eine bestehende Organisationsgruppe, einen Filter oder ein Ressourcenziel angeben. Sie können jedoch auch individuelle Ressourcen auswählen.

   Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.
4. Geben Sie im Bereich "Zeitplanungshinweise" den geplanten Zeitpunkt bzw. Zeitraum für die Installation an und wählen Sie die gewünschten Optionen aus.
5. Klicken Sie auf "Änderungen speichern".

Anzeigen des Installationsstatusberichts

Der Installationsstatusbericht zeigt Details aller Symantec Management-Agent-Push-Installationsversuche an. Der Bericht umfasst nicht die Details von Pull-Installationen.

Standardmäßig werden Details aller Installationsversuche der letzten Woche aufgelistet. Sie können den Zeitraum angeben, um die Ergebnisse nach Computernamen und Domäne anzuzeigen und zu filtern.

Diese Aufgabe ist ein Schritt in den folgenden Vorgängen:

- Installieren des Symantec Management-Agent unter Windows
  Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.
- Manuelles Installieren des Symantec Management-Agent unter UNIX, Linux und MacOS

Siehe "Manuelle Installation von Symantec Management Agent auf UNIX-, Linux- und Mac-Computern" auf Seite 266.

So zeigen Sie den Bericht "Agent-Installationsstatus" an

1. Wählen Sie in der Symantec Management Console im Menü "Aktionen" die Option "Agents/Plugins > Symantec Management-Agent - Push".
2. Klicken Sie auf der Seite "Symantec Management-Agent – Installation" auf "Statusbericht".

   Der Bericht zeigt alle Push-Installationsversuche für den Symantec Management-Agent und den Symantec Management-Agent für UNIX, Linux und Mac an. Derselbe Bericht ist auch über die Registerkarten "Agent installieren" und "Agent für UNIX, Linux und Mac installieren" verfügbar.
3. Zeigen Sie im Fenster "Agent-Installationsstatus" die Details jedes Installationsversuchs an.
4. (Optional) Wenn Sie den Zeitraum ändern oder die Ergebnisse nach Computernamen und Domäne filtern möchten, können Sie unter "Parameter" die passenden Benutzerparameter festlegen:

Anzeigen	Geben Sie den gewünschten Zeitraum an. Geben Sie die entsprechende Anzahl von Einheiten (Stunden, Tage, Wochen oder Monate) in den Feldern "Von" und "Bis" ein.
Einheiten	Geben Sie die Einheiten an, die Sie für die Werte für "Anzeigen" benutzen möchten.
Filtern nach	Wenn Sie die Ergebnisse nach Computernamen oder Domäne (oder beide) filtern möchten, geben Sie den entsprechenden Filtertext in den Feldern an.

5. (Optional) Wenn Sie die Benutzerparameter geändert haben, klicken Sie auf "Aktualisieren", um die aktualisierten Berichtergebnisse anzuzeigen.

Anzeigen und Verwalten des Agent-Registrierungsstatus

Anhand des Berichts "Agent-Registrierungsstatus" können Sie alle Registrierungsanforderungen und abgeschlossene Registrierungen von Symantec Management-Agents anzeigen.

Diesem Bericht können Sie entnehmen, welche Computer von der "Agent-Registrierungsrichtlinie" automatisch zugelassen oder blockiert wurden. Beachten Sie, dass die Registrierung für eine direkte Symantec Management-Agent-Push-Installation umgangen wird. Jedoch werden die Computer weiterhin im Bericht angezeigt und ihr Status ist auf "Zugelassen" eingestellt. Wenn

keine Agent-Registrierungsrichtlinie für den Computer gilt, ist sein Status auf "Ausstehend" eingestellt und über das Kontextmenü können Sie ihn manuell zulassen oder blockieren. Im Kontextmenü können Sie das Vertrauen der zuvor zugelassenen Agents auch widerrufen.

Siehe "Erstellen einer Agent-Registrierungsrichtlinie" auf Seite 253.

Eingehende Registrierunganforderungen werden anhand der Ressourcenschlüssel unterschieden, die entsprechend der Ressourcenschlüsselsuche zusammengeführt werden.

In manchen Situationen werden möglicherweise doppelte Registrierungsanforderungen angezeigt. Beispiel: Wenn Sie den Agent auf einem Computer, der bereits auf Notification Server registriert ist, erneut installieren, ändert sich sein öffentlicher Schlüssel. In diesem Fall empfiehlt Symantec, dass Sie die Registrierungsanforderung genehmigen, damit dieser Computer die Kommunikation mit Notification Server fortsetzen kann. Die doppelten Registrierungsanforderungen werden möglicherweise angezeigt, wenn Sie Computer mit identischen Ressourcenschlüsseln in Ihrem Netzwerk haben. In diesem Fall empfiehlt Symantec, die doppelte Registrierungsanforderung nicht zu genehmigen, weil dies möglicherweise zu Konnektivitätsproblemen für die zuvor existierende Ressource führt.

Wenn Sie doppelte Registrierungsanforderungen in Ihrem Bericht haben, werden die Anforderungen wie folgt verarbeitet:

- Wenn die Erstanforderung und auch die doppelte Anforderung zugelassen ist, wird die doppelte Anforderung mit der bestehenden Ressource zusammengeführt. Der Bericht wird entsprechend aktualisiert, dass ein einzelner Eintrag angezeigt wird.
- Wenn die Erstanforderung zugelassen, aber die doppelte Anforderung blockiert ist, bleiben beide Anforderungen in der Liste. Die zugelassene Anforderung stellt die tatsächliche Ressource und die doppelte Anforderung mit dem Status "Blockiert" oder "Ausstehend" stellt den Registrierungsversuch von einer möglicherweise doppelten Ressource dar.

Im Bericht "Agent-Registrierungsstatus" werden alle Anforderungen für Prüfungszwecke aufbewahrt und können kontinuierlich beobachtet werden.

Diese Aufgabe ist ein Schritt in den folgenden Prozessen:

- Installieren des Symantec Management-Agent auf Windows-Computern. Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.
- Manuelles Installieren des Symantec Management-Agent auf UNIX-, Linux- und Mac-Computern.

Siehe "Manuelle Installation von Symantec Management Agent auf UNIX-, Linux- und Mac-Computern" auf Seite 266.

So zeigen Sie den Agent-Registrierungsstatus an und verwalten ihn

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Erweitern Sie im linken Teilfenster unter "Berichte" die Optionsfolge "Notification Server Management > Registrierung" und klicken Sie anschließend auf "Agent-Registrierungsstatus".

3 (Optional) Ändern Sie auf der Seite "Agent-Registrierungsstatus" mit den Kontextmenüoptionen den Agent-Status. Beachten Sie, dass die Kontextmenüoptionen je nach Agent-Status unterschiedlich sein können.

Zulassen	Sie können die Agents zulassen, die sich im Status "Ausstehend", "Blockiert" oder "Widerrufen" befinden. Wenn Sie einen blockierten Agent zulassen, wird das Vertrauen beim nächsten Mal gewährt, wenn der Agent eine Registrierungsanforderung an Notification Server sendet.
Blockieren	Sie können die Agents blockieren, die sich im Status "Ausstehend" oder "Widerrufen" befinden. Wenn Sie einen widerrufenen Computer blockieren, ändert sich sein Funktionsstatus nicht. Durch Ändern des Status können Sie jedoch die widerrufenen Computer unterscheiden, die niemals mehr von den widerrufenen Computern aus, die möglicherweise weiterhin Ihre Aufmerksamkeit erfordern, eine Verbindung zu Notification Server herstellen sollten. Hinweis: Computer mit dem Status "Blockiert" werden nach einem vordefinierten Zeitraum aus der Liste entfernt, wenn während dieser Zeit keine neuen Registrierungsanforderungen von demselben Computer gesendet wurden. Der Standardzeitraum beträgt drei Monate, aber Sie können ihn auf der Seite "Bereinigungseinstellungen" ändern.

Widerrufen	Sie können die Registrierung der Agents widerrufen, die Sie vorher zugelassen haben. Beispielsweise können Sie die Registrierung für den Clientcomputer widerrufen, der als fehlend oder gestohlen gemeldet ist. Nachdem Sie den Agent widerrufen haben, erhält er keine Richtlinien mehr vom Notification Server. Ein widerrufener Computer kann auch nicht als Site Server verwendet werden. Während des Widerrufens des internen Agent-Vertrauens, wird die Schlüsselregistrierung der Agent-Verschlüsselung auf dem Notification Server als widerrufen markiert. Widerrufene Agents erhalten keine Richtlinien und führen keine Aufgaben aus. Außerdem löscht der widerrufene Agent lokal gespeicherte Richtlinien, um seine Aktivität zu minimieren. Nach dem Widerrufen ist der Symantec Management-Agent gezwungen, den Registrierungsvorgang erneut zu starten. Der Agent erhält Informationen über seinen widerrufenen Status, wenn er das nächste Mal auf gesicherte Daten zuzugreifen versucht. Der Notification Server benachrichtigt den Agent nicht über das Widerrufen, wenn es auftritt. Hinweis: Der widerrufene Agent bleibt im Status ´"Widerrufen", selbst wenn die Agent-Registrierungsrichtlinie ihn zulässt. Sie müssen die widerrufenen Computer manuell verwalten, wenn Sie ihren Status ändern möchten.

Manuelle Installation von Symantec Management Agent auf UNIX-, Linux- und Mac-Computern

Sie können den Symantec Management-Agent mit einer manuellen Push- oder Pull-Installation installieren. Er wird empfohlen, den Symantec Management-Agent über eine manuelle Push-Installation auf ausgewählten Computern zu installieren. Befindet sich der Remote-Computer hinter einer Firewall oder hat er nur begrenzten Netzwerkzugriff, müssen Sie möglicherweise eine manuelle Pull-Installation ausführen.

Siehe "Infos zu Symantec Management-Agent" auf Seite 246.

Tabelle 15-4 Vorgang zur manuellen Installation von Symantec Management Agent auf UNIX-, Linux- und Mac-Computern

Schritt	Aktion	Beschreibung
Schritt 1	Wählen Sie die Computer aus, auf denen Sie den Agent und die Plugins installieren möchten.	Sie haben die folgenden Optionen für das Auswählen von Computern: ■ Network Discovery ■ Manuelle Auswahl durch Hinzufügen von Client-Hostnamen oder IP-Adressen ■ Active Directory-Import ■ Import unter Verwendung einer Datei mit kommagetrennten Werten.
Schritt 2	Überprüfen Sie, dass die Computer die Installationsvoraussetzungen erfüllen.	Jeder Computer muss die Hardware- und Softwarevoraussetzungen erfüllen, bevor Sie den Symantec Management-Agent auf ihm installieren können. Siehe "Installationsanforderungen für den Symantec Management Agent für UNIX, Linux und Mac" auf Seite 269.
Schritt 3	(Optional) Definieren Sie die Agent-Registrierungsrichtlinien.	Nachdem Sie Symantec Management Agent installiert haben, sendet das Programm eine Registrierungsanfrage an den Notification Server, um die Vertrauensstellung zwischen dem Server und dem Client herzustellen. Die Standardregistrierungsrichtlinie für Agents ermöglicht die automatischer Registrierung aller Agents. Sie können die Standardrichtlinie ändern oder kundenspezifische Richtlinien erstellen, um einschränkendere Regeln anzugeben. Siehe "Erstellen einer Agent-Registrierungsrichtlinie" auf Seite 253.
Schritt 4	Geben Sie die Installationseinstellungen an.	Mit Installationseinstellungen für UNIX, Linux und Mac können Sie die Kommunikations- und die Authentifizierungseinstellungen für den Symantec Management-Agent für UNIX, Linux und Mac konfigurieren. Wenn Sie Computernamen aus einer CSV-Datei importieren, können Sie diese Einstellungen in der CSV-Datei angeben. Sie können diese Einstellungen auch über die Symantec Management Console festlegen oder ändern. Siehe "Angeben der Installationseinstellungen für den Symantec Management-Agent für UNIX, Linux und Mac " auf Seite 271.

Schritt	Aktion	Beschreibung
Schritt 5	Installieren Sie den Symantec Management-Agent mit dem geeigneten Verfahren.	Das bevorzugte Verfahren ist eine Push-Installation von Symantec Management-Agent auf den ausgewählten Computern. Wenn sich ein Computer jedoch hinter einer Firewall befindet oder schwer für den Notification Server zu erreichen ist, können Sie stattdessen eine Pull-Installation des Symantec Management-Agent durchführen. Siehe "Installieren von Symantec Management-Agent für UNIX Linux und Mac mit einer manuellen Push-Installation" auf Seite 272. Siehe "Installieren von Symantec Management-Agent unter UNIX, Linux und Mac OS mit einer manuellen Pull-Installation" auf Seite 276.
Schritt 6	Zeigen Sie den Agent-Registrierungsstatus an und verwalten Sie ihn, um die erfolgreiche Registrierung zu prüfen.	Der Bericht "Agent-Registrierungsstatus" ermöglicht es, alle Registrierungsanfragen und abgeschlossenen Registrierungen von Symantec-Management Agents anzuzeigen und zu verwalten. Siehe "Anzeigen und Verwalten des Agent-Registrierungsstatus" auf Seite 261.

Erstellen einer CSV-Datei zum Importieren von UNIX-, Linux- und Mac-Computern

Wenn Sie Symantec Management-Agent für UNIX, Linux und Mac auf vielen Computern installieren möchten, die verschiedene Verbindungs- und Konfigurationseinstellungen erfordern, empfehlen wir, eine CSV-Datei zum Importieren der Computer und Konfigurieren der Installationseinstellungen zu verwenden. Die CSV-Datei ist eine kommagetrennte Textdatei, die die DNS-Namen oder IP-Adressen der Clientcomputer enthält, auf denen der Symantec Management-Agent installiert werden soll. Jede Zeile in der CSV-Datei steht für einen Computer, der in die Seite "Symantec Management-Agent installieren" importiert wird. Die CSV-Datei kann auch die Installationseinstellungen für jeden Computer enthalten.

Siehe "Installieren von Symantec Management-Agent für UNIX Linux und Mac mit einer manuellen Push-Installation" auf Seite 272.

Eine CSV-Vorlagendatei zum Importieren von UNIX-, Linux- und Mac-Computern (`CSVTemplate.csv`) ist im Lieferumfang der Symantec Management-Plattform enthalten. Die Spaltenüberschrift der CSV-Vorlage gibt die erforderlichen Daten sowie die gültigen Werte an.

Warnung: Das Listentrennzeichen der CSV-Datei muss den Regionaleinstellungen des Servers entsprechen. Beispiel: Die Beispielsdatei `CSVTemplate.csv` hat die Regionaleinstellung "English (United States)" mit Komma (,) als Trennzeichen. Sie können die regionalen Einstellungen der Symantec Management-Plattform in Windows Systemsteuerung anzeigen.

Diese Aufgabe ist ein Schritt beim manuellen Installieren des Symantec Management-Agent.

Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.

So erstellen Sie eine CSV-Datei zum Importieren von UNIX-, Linux- und Mac-Computern

1. Wählen Sie in der Symantec Management Console im Menü "Aktionen" die Option "Agents/Plugins > Symantec Management-Agent - Push".
2. Klicken Sie auf der Seite "Symantec Management-Agent installieren" auf der Registerkarte "Agent für UNIX, Linux and Mac installieren" unter "Rollout von Agent für UNIX, Linux und Mac auf Computer" mit der rechten Maustaste auf "CSV-Dateivorlage" und wählen Sie im Kontextmenü die Option "Ziel speichern unter".
3. Geben Sie im Dialogfeld "Speichern unter" einen geeigneten Dateinamen für die Datei `"CSVTemplate.csv"` ein, öffnen Sie den entsprechenden Ordner und klicken Sie dann auf "Speichern".
4. Öffnen Sie die gespeicherte CSV-Datei in einem Texteditor und geben Sie die Informationen für jeden Computer ein, auf dem Sie Symantec Management-Agent für UNIX, Linux und Mac installieren möchten.

   Sie müssen nicht alle Felder verwenden. Sie können nur die benötigten Felder benutzen, wie z. B. Computername, Root-name, Root-Kennwort usw.

   Die Einstellungen, die Sie in der CSV-Datei angeben können, entsprechen den Einstellungen, die Sie im Dialogfeld "Installationseinstellungen" in der Symantec Management Console festlegen können.
5. Speichern Sie die CSV-Datei, wenn Sie alle Einstellungen angegeben haben.

Installationsanforderungen für den Symantec Management Agent für UNIX, Linux und Mac

Der Computer muss die Hardware- und Softwareanforderungen erfüllen, bevor Sie den Symantec Management-Agent für UNIX, Linux und Mac installieren können.

Siehe "Methoden für das Installieren des Symantec Management-Agent" auf Seite 248.

Diese Aufgabe ist ein Schritt beim manuellen Installieren des Symantec Management-Agent.

Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.

Tabelle 15-5 Installationsanforderungen des Symantec Management-Agent für UNIX, Linux und Mac

Voraussetzung	Beschreibung
Betriebssystem	Eines der folgenden Betriebssysteme: ■ Solaris 9 (SPARC) ■ Solaris 10 (x86, x86_64 und SPARC) ■ Red Hat Enterprise Linux 5.0, 5.1, 5.2, 5.3, 5.4, 5.5, 5.6, 5.7, 5.8, 5.9 (x86 und x86_64) ■ Red Hat Enterprise Linux 6.0, 6.1, 6.2, 6.3, 6.4 (x86 und x86_64) ■ SUSE Linux Enterprise Server 10, 11 SP1, 11 SP2 (x86 und x86_64) ■ SUSE Linux Enterprise Desktop 10, 11 SP1, 11 SP2 (x86 und x86_64) ■ MacOS X 10.6.x, 10.7.x, 10.8.x (Universal Binary) ■ MacOS X Server 10.6.x, 10.7.x, 10.8.x (Universal Binary) ■ HP-UX 11.11 (PA-RISC), 11.23 (PA-RISC/IA64), 11.31 (PA-RISC/IA64) ■ AIX 6.1 PPC, 7.1 Standard
Festplattenspeicher	60 MB
RAM	Mindestens 25 MB
Zugriffsrechte	Unter UNIX und Linux sind Root-Benutzerrechte erforderlich. Für Mac OS X sind administrative oder Root-Benutzerrechte erforderlich.
Remote SSH-Verbindungen aktiviert	Remote SSH-Verbindungen müssen aktiviert werden. Es muss einen SSH-Server auf dem Clientcomputer ausgeführt werden und die Firewall muss konfiguriert werden, um eine eingehende SSH-Verbindung zuzulassen.
Ausgehende Verbindung zum Notification Server	Die Firewall muss konfiguriert werden, um eine ausgehenden Verbindung zu einem WEB-Port auf Notification Server zuzulassen.

Angeben der Installationseinstellungen für den Symantec Management-Agent für UNIX, Linux und Mac

Bei den Installationseinstellungen handelt es sich um Einstellungen zu Kommunikation und Authentifizierung für den Symantec Management-Agent für UNIX, Linux und Mac. Sie müssen den erforderlichen privilegierten Kontoanmeldenamen und sein Kennwort für jeden Zielcomputer angeben.

Siehe "Installieren von Symantec Management-Agent für UNIX Linux und Mac mit einer manuellen Push-Installation" auf Seite 272.

Wenn Sie Computer aus einer CSV-Datei importieren, können Sie die erforderlichen Installationseinstellungen für jeden Computer in der CSV-Datei angeben. Wenn Sie keine Einstellungen in der CSV-Datei angeben oder wenn Sie Computer manuell hinzugefügt haben, müssen Sie die erforderlichen Einstellungen für jeden Zielcomputer angeben, bevor Sie den Symantec Management-Agent für UNIX, Linux und Mac installieren.

Sie können Installationseinstellungen für einen bestimmten Computer oder für mehrere Computer angeben. Wenn Sie mehrere Computer auswählen, werden die gleichen Installationseinstellungen auf jeden Computer angewendet. Sie können die aktuellen Installationseinstellungen von einem Computer duplizieren und auf andere Computer anwenden.

Siehe "Erstellen einer CSV-Datei zum Importieren von UNIX-, Linux- und Mac-Computern" auf Seite 268.

Diese Aufgabe ist ein Schritt beim manuellen Installieren des Symantec Management-Agent.

Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.

So geben Sie Installationseinstellungen für Symantec Management-Agent für UNIX-, Linux- und Mac an

1. Wählen Sie in der Symantec Management Console im Menü "Aktionen" die Option "Agents/Plugins > Symantec Management-Agent - Push".
2. Klicken Sie auf der Seite "Symantec Management-Agent installieren" auf der Registerkarte "Agent für UNIX, Linux und Mac installieren" unter "Rollout von Agent für UNIX, Linux und Mac auf Computern" in der Computerliste auf den Computer, für den Sie die Installationseinstellungen für Symantec Management-Agent ändern möchten, und klicken Sie dann auf "Installationseinstellungen".

   Sollen identische Installationseinstellungen für mehrere Computer gelten oder die aktuellen Installationseinstellungen von einem anderen Computer dupliziert werden, wählen Sie die entsprechenden Computer aus.

3 (Optional) Wenn Sie die aktuellen Installationseinstellungen von einem bestimmten Computer duplizieren möchten, wählen Sie den gewünschten Computer im Dialogfeld "Installationseinstellungen" in der Dropdown-Liste "Einstellungen laden" aus.

   Die Option "Einstellungen laden" wird an dem rechten oberen Rand des Dialogfelds "Installationseinstellungen" angezeigt, wenn Sie mehrere Computer ausgewählt haben.

4 Geben Sie die Installationseinstellungen für die ausgewählten Computer an.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.

5 Klicken Sie im Dialogfeld "Installationseinstellungen" auf "OK".

Installieren von Symantec Management-Agent für UNIX Linux und Mac mit einer manuellen Push-Installation

Sie können eine Push-Installation von Symantec Management-Agent für UNIX, Linux und Mac auf den Computern ausführen, die auf der Seite "Symantec Management-Agent installieren" aufgelistet sind.

Bevor Sie Symantec Management-Agent von der Seite "Symantec Management-Agent installieren" manuell installieren oder deinstallieren können, müssen Sie die entsprechenden Computer auswählen. Sie können die Computer auswählen, die mit der Ressourcenerkennung gefunden wurden, die Computernamen manuell eingeben oder die Computer aus einer CSV-Datei importieren.

Hinweis: Sie können den Symantec Management-Agent nur auf den Computern manuell installieren, die unter Verwendung der Domänen-Ressourcenerkennung oder der Netzwerkerkennung erkannt wurden.

Die Push-Installation des Symantec Management-Agent für UNIX, Linux und Mac wird vom Symantec Management-Plattform-Computer ausgeführt. Der Symantec Management-Plattform-Computer erstellt eine Verbindung mit dem Ziel-UNIX-, Linux- oder Mac-Computer, lädt die erforderlichen Dateien hoch und führt sie dann auf dem Zielcomputer aus.

Die Installation läuft wie folgt ab:

- Die Symantec Management-Plattform versucht, eine Verbindung mit dem Zielcomputer über SSH herzustellen.
  Das SSH-Protokoll unterstützt die Anmeldung mit privilegierten oder nicht autorisierten Benutzerkonten und mehreren Kennwörtern.

- Wenn eine Verbindung hergestellt wurde, ermittelt die Symantec Management-Plattform das Betriebssystem und die Umgebung des Clientcomputers. Danach startet sie das entsprechende plattformabhängige Push-Installationsskript.
- Das Push-Installationsskript erstellt eine Verzeichnisstruktur auf dem Clientcomputer und versucht dann das Dienstprogramm `aex-bootstrap` vom Symantec Management-Plattform-Computer herunterzuladen. Das Push-Installationsskript versucht jede der folgenden Methoden, in der gegebenen Reihenfolge, bis eine erfolgreich ist: SCP/SFTP, wget, curl.
  Wenn alle diese Methoden fehlschlagen, verwendet das Skript den dd-Befehl, um das aex-bootstrap.Z.uu-Archiv auf den Zielcomputer zu übertragen. Danach benutzt es uudecode, um das Archiv in ein natives Format zu konvertieren.
- Die Datei `".aex-agent-install-config.xml"`, die alle Symantec Management-Agent-Installationseinstellungen enthält, wird auf den Clientcomputer heruntergeladen.
- Das Skript `aex-bootstrap` wird ausgeführt und die Verbindung zur Symantec Management-Plattform wird geschlossen.
- Das Skript `"aex-bootstrap` lädt den Rest des Symantec Management-Agent vom Symantec Management-Plattform-Computer herunter und konfiguriert den Agent mit den Einstellungen aus der Datei `".aex-agent-install-config.xml"`.
- Wenn der Symantec Management-Agent für UNIX, Linux und Mac das erste Mal ausgeführt wird, wird ein Grundinventar erfasst und an die Symantec Management-Plattform gesendet.
- Der Symantec Management-Agent für UNIX, Linux und Mac erhält die entsprechenden Aufgaben und Richtlinien von der Symantec Management-Plattform.

Hinweis: Drittanbieter-Firewalls müssen so konfiguriert werden, dass eine SSH-Verbindung von Symantec Management-Plattform an den ULM-Client möglich ist und eine manuelle Push-Installation funktioniert. Die Firewallkonfiguration sollte die gleichen Identifikationsdaten verwenden, die Sie in Schritt 4 im Dialogfeld "Installationseinstellungen" eingegeben haben.

Diese Aufgabe ist ein Schritt beim manuellen Installieren des Symantec Management-Agent.

Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.

So installieren Sie Symantec Management-Agent für UNIX Linux und Mac mit einer manuellen Push-Installation

1. Wählen Sie in der Symantec Management Console im Menü "Aktionen" die Option "Agents/Plugins > Symantec Management-Agent - Push".
2. Wählen Sie auf der Seite "Symantec Management-Agent installieren" auf der Registerkarte "Agent for UNIX, Linux und Mac installieren" unter "Rollout von Agent für UNIX, Linux und Mac auf Computer" die UNIX-, Linux- und MacOS-Computer aus, auf denen Symantec Management-Agent installiert werden soll:

So fügen Sie einen Computer manuell hinzu	Geben Sie im Textfeld den Computernamen (muss ein auflösbarer DNS-Name sein) oder die IP-Adresse ein und klicken auf dann "Hinzufügen".
So wählen Sie aus den verfügbaren Computern aus	Klicken Sie auf "Computer auswählen" im Dialogfeld "Computer auswählen", fügen Sie die entsprechenden Computer aus der Liste "Verfügbare Computer" der Liste "Ausgewählte Computer" hinzu und klicken Sie dann auf "OK".

So importieren Sie Computer aus einer CSV-Datei

1. Klicken Sie in der Symbolleiste auf "Computer aus einer ausgewählten Datei importieren".
2. Wählen Sie im Dialogfeld "Zu importierende Datei auswählen" die gewünschte CSV-Datei aus und klicken Sie auf "Öffnen".

Die CSV-Datei ist eine kommagetrennte Textdatei. Die Datei enthält die DNS-Namen oder die IP-Adressen der Clientcomputer, auf denen der Symantec Management-Agent installiert werden soll. Für UNIX-, Linux- und MacOS-Computer stellt jede Zeile in der CSV-Datei einen Computer dar, der in die Seite "Symantec Management-Agent installieren" importiert wird. Sie können auch die erforderlichen Installationseinstellungen in die CSV-Datei aufnehmen. Mit diesen Installationseinstellungen können Sie die Kommunikations- und die Authentifizierungseinstellungen für Symantec Management-Agent für UNIX, Linux und Mac konfigurieren.

Wenn Sie viele Computer haben, die verschiedene Verbindungs- und Konfigurationseinstellungen erfordern, verwenden Sie eine CSV-Datei, um die Computer zu importieren.

Siehe "Erstellen einer CSV-Datei zum Importieren von UNIX-, Linux- und Mac-Computern" auf Seite 268.

3. Klicken Sie auf "Installationseinstellungen" und geben Sie dann im Dialogfeld "Installationseinstellungen" die entsprechenden Installationseinstellungen an.

   Wenn Sie Computer manuell hinzugefügt haben, müssen Sie die erforderlichen Installationseinstellungen für jeden Zielcomputer vor der Installation von Symantec Management-Agent für UNIX, Linux und Mac angeben. Wenn Sie Computer aus einer CSV-Datei importiert haben, haben Sie evtl. die erforderlichen Installationseinstellungen für jeden Computer bereits in der CSV-Datei angeben. Sie können diese Einstellungen für einzelne Computer oder Computergruppen ändern.

   Siehe "Angeben der Installationseinstellungen für den Symantec Management-Agent für UNIX, Linux und Mac " auf Seite 271.

4. (Optional) Geben Sie in das Feld "Simultane Aufgaben" die Anzahl der Installationen ein, die gleichzeitig ausgeführt werden sollen.

   Dieser Wert definiert die Anzahl der parallel ausgeführten Threads für die Push-Installation von Symantec Management-Agent. Alle Threads nutzen eine gemeinsame Warteschlange von der sie den nächsten Computer entnehmen, um die Installation auf ihm durchzuführen. Der Standardwert ist 5, aber Sie sollten einen anderen Wert verwenden, um der Leistung der Symantec Management-Plattform, der Clientcomputer und der Netzwerkkapazität anzupassen. Das Erhöhen der Anzahl gleichzeitiger Aufgaben kann die Gesamtinstallationszeit reduzieren.

5. Klicken Sie auf "Installieren".

6. Aktivieren Sie im Dialogfeld "Push-Installation" das Kontrollkästchen, um der Softwareinstallation von Drittanbietern zuzustimmen, und klicken Sie dann auf "OK".

   Hinweis: Wenn die Zielplattform 64-Bit RHEL 6.0 oder höher ist und keine 32-Bit Compatibility Layer installiert ist, schlägt die Agent-Push-Installation fehl, wenn Sie der Softwareinstallation von Drittanbietern nicht zustimmen.

   Die Spalte "Status" in der Computerliste zeigt auf jedem Computer an, ob die Installation erfolgreich war oder fehlgeschlagen ist. Beachten Sie, dass der neu installierte Symantec Management Agent seinen Status dem ursprünglichen Notification Server meldet, selbst wenn ein anderer Notification Server ihn verwaltet.

7. Wenn die Computerliste nicht automatisch in der Symbolleiste aktualisiert wird, klicken Sie auf "Aktualisieren", um den aktuellen Push-Installationsstatus für jeden Computer anzuzeigen.

Installieren von Symantec Management-Agent unter UNIX, Linux und Mac OS mit einer manuellen Pull-Installation

Falls SSH nicht verfügbar ist oder falls Sie Symantec Management-Agent für UNIX, Linux und Mac auf Remote-Computern installieren möchten, die begrenzten Netzwerkzugriff haben, oder die Zielcomputer sich hinter einer Firewall befinden, können Sie Symantec Management-Agent per Pull-Installation installieren. Sie oder ein Benutzer mit Administratorrechten können bzw. kann sich bei jedem Computer einloggen, über eine URL auf Symantec Management-Plattform zugreifen und das Bootstrap-Installationsprogramm herunterladen, das Symantec Management-Agent unter UNIX, Linux und Mac OS installiert.

Die URL der Seite "Symantec Management-Agent für UNIX, Linux und Mac herunterladen" wird auf der "Symantec Management-Agent - Installationsseite" unter "URL der Downloadseite für UNIX-, Linux- und Mac-Benutzer" angezeigt. Sie können die Seite anzeigen, nicht jedoch diese Einstellung ändern.

Siehe "Infos zu Symantec Management-Agent" auf Seite 246.

Siehe "Problemlösungsbefehle für Symantec Management-Agent für UNIX, Linux und Mac" auf Seite 533.

Diese Aufgabe ist ein Schritt im Vorgang zur manuellen Installation von Symantec Management Agent.

Siehe "Installieren des Symantec Management-Agent unter Windows" auf Seite 250.

So zeigen Sie die Seite "Symantec Management-Agent für UNIX, Linux und Mac herunterladen" in der Vorschau an

1. Klicken Sie in Symantec Management Console im Menü "Aktionen" auf "Agents/Plugins > Symantec Management-Agent - Push".
2. Klicken Sie auf der Seite "Symantec Management-Agent - Installation" auf der Registerkarte "Installation von Symantec Management Agent für UNIX, Linux und Mac" unter "URL der Downloadseite für UNIX-, Linux- und Mac-Benutzer" in der Dropdown-Liste "Plattform auswählen" auf die entsprechende Plattform und klicken Sie auf "Seite anzeigen".

So führen Sie eine Pull-Installation von Symantec Management-Agent für UNIX, Linux und Mac auf einem Remote-Computer durch

1. Loggen Sie sich am Remote-Computer als Administrator ein.
2. Öffnen Sie auf dem Remote-Computer einen Webbrowser und rufen Sie dann folgende URL auf:

   http://*SMPName*/Altiris/UnixAgent/AltirisUnixAgentDownload.aspx?ID=*Platform*

   Dabei entspricht *"SMPName"* dem Namen Ihres Symantec Management-Plattform-Computers und *"Plattform"* der entsprechenden Plattform.
3. Befolgen Sie die Anweisungen für das Herunterladen und Ausführen des Bootstrap-Installationsprogramms auf dem Remote-Computer, die auf der Seite "Symantec Management-Agent für UNIX, Linux und Mac herunterladen" angezeigt werden.

Kapitel 16

Aktualisieren und Deinstallieren des Symantec Management Agent

In diesem Kapitel werden folgende Themen behandelt:

- Methoden für das Aktualisieren des Symantec Management-Agent
- Methoden für das Deinstallieren des Symantec Management-Agent
- Konfigurieren von Aktualisierungs- und Deinstallationsrichtlinien für den Symantec Management-Agent
- Informationen zur Legacy-Agent-Kommunikation
- Konfigurieren des Symantec Management-Agent-Pakets
- Manuelles Entfernen des Symantec Management-Agent unter Windows

Methoden für das Aktualisieren des Symantec Management-Agent

Sie müssen die richtige Version des Symantec Management-Agent auf Ihren verwalteten Computern installieren. Wenn auf einem Computer noch eine ältere Version installiert ist, sollten Sie ein Upgrade durchführen.

Siehe "Infos zu Symantec Management-Agent" auf Seite 246.

Tabelle 16-1 Methoden zum Aktualisieren des Symantec Management-Agent

Methode	Beschreibung
Manuelle Push-Installation des Symantec Management-Agent auf den entsprechenden Computern.	Sie können ein Upgrade des Symantec Management-Agent manuell durchführen, indem Sie eine Push-Installation auf den entsprechenden Computern ausführen. Sie können eine Push-Installation auf Computern durchführen, auf denen eine ältere Version des Symantec Management-Agent installiert ist. Siehe "Installieren des Symantec Management-Agent für Windows mit einer manuellen Push-Installation" auf Seite 256. Siehe "Installieren von Symantec Management-Agent für UNIX Linux und Mac mit einer manuellen Push-Installation" auf Seite 272.
Verwenden Sie die Symantec Management-Agent-Upgraderichtlinie.	Die Aktualisierungsrichtlinie für den Symantec Management-Agent ist im Lieferumfang von Notification Server enthalten. Sie können diese Richtlinie aktivieren und so konfigurieren, dass auf allen verwalteten Computern die richtige Version des Symantec Management-Agent installiert wird. Siehe "Konfigurieren von Aktualisierungs- und Deinstallationsrichtlinien für den Symantec Management-Agent" auf Seite 280. **Hinweis:** Wenn Sie IT Management Suite von einer früheren Version auf 7.5 aktualisieren und der Modus "Legacy-Agent-Kommunikation" (LAC) aktiviert ist, kann ein aktualisierter Notification Server einen begrenzten Satz an Verwaltungsaufgaben auf Endgeräten mit älteren Versionen des Symantec Management-Agent ausführen. Sie können den Modus "Legacy-Agent-Kommunikation" in der Symantec Management Console auf der Seite "Notification Server-Einstellungen" auf der Registerkarte "Verarbeitung" verwalten. Siehe "Informationen zur Legacy-Agent-Kommunikation" auf Seite 284. Siehe "Konfigurieren von Notification Server-Einstellungen" auf Seite 68.

Methoden für das Deinstallieren des Symantec Management-Agent

Sie können den Symantec Management-Agent von einem verwalteten Computer entfernen, wenn Sie ihn nicht mehr benötigen. Sie müssen die auf dem Computer installierten Lösungs-Agents nicht deinstallieren. Dies geschieht automatisch bei der Deinstallation des Symantec Management-Agent.

Siehe "Infos zu Symantec Management-Agent" auf Seite 246.

Tabelle 16-2 Methoden für das Deinstallieren des Symantec Management-Agent

Methode	Beschreibung
Manuelle Deinstallation.	Die manuelle Deinstallation wird von der Symantec Management Console aus eingeleitet und deinstalliert Symantec Management-Agent sofort. Sie können Symantec Management-Agent mit dem gleichen Deinstallationsvorgang auf beliebig vielen Windows-Computern deinstallieren. Außerdem können Sie die Deinstallationsoptionen für die einzelnen Deinstallationen anpassen. Diese Option ist für nur Windows-Computer verfügbar. Siehe "Manuelles Entfernen des Symantec Management-Agent unter Windows" auf Seite 286.
Verwenden Sie die Symantec Management-Agent-Deinstallationsrichtlinie	Die Symantec Management-Agent-Deinstallationsrichtlinie ist im Lieferumfang der Symantec Management-Plattform enthalten. Sie können diese Richtlinie aktivieren und so konfigurieren, dass Symantec Management-Agent von den gewünschten Computern entfernt wird. Diese Option ist sowohl für Windows- als auch UNIX-, Linux- und Mac-Computer verfügbar. Siehe "Konfigurieren von Aktualisierungs- und Deinstallationsrichtlinien für den Symantec Management-Agent" auf Seite 280.

Konfigurieren von Aktualisierungs- und Deinstallationsrichtlinien für den Symantec Management-Agent

Sie können die Richtlinien für das Aktualisieren und Deinstallieren des Symantec Management-Agent Ihren Anforderungen entsprechend konfigurieren. Beide

Richtlinien nutzen das entsprechende Symantec Management-Agent-Paket, aber unterschiedliche Programme.

Siehe "Infos zu Symantec Management-Agent" auf Seite 246.

Notification Server stellt einige Standardfilter zur Verfügung, die Sie für geplante Agent-Installationen sowie Aktualisierungs- und Deinstallationsrichtlinien für den Agent verwenden können. Diese Filter sind im Symantec Management-Agent-Ordner im entsprechenden Unterordner abgelegt. Sie können die Standardfilter nicht ändern. Sie können sie jedoch duplizieren und daraus neue Filter erstellen, die Sie dann Ihren Anforderungen entsprechend bearbeiten können.

Jedoch müssen Sie achtgeben, wenn Sie den Symantec Management-Agent basierend auf Ressourcenzielen aktualisieren. In einer großen Umgebung kann es sinnvoller sein, die Aktualisierungen zu staffeln. Verwenden Sie zunächst ein Testziel und staffeln Sie dann das Rollout an geeignete Ziele. Es kann zum Beispiel gewisse Probleme mit dem Upgrade geben. Daher ist es sinnvoll, es auf einer kleinen Computergruppe zu testen und die Probleme zu lösen, bevor sie auf alle Computer verteilt werden. Außerdem verringert eine gestaffelte Aktualisierung die Netzwerkbelastung, da die Agents normalerweise Daten vom Notification Server anfordern müssen, sobald sie aktualisiert wurden.

Hinweis: Wenn Sie IT Management Suite von einer früheren Version auf 7.5 aktualisieren und der Modus "Legacy-Agent-Kommunikation" (LAC) aktiviert ist, kann ein aktualisierter Notification Server einen begrenzten Satz an Verwaltungsaufgaben auf Endgeräten mit älteren Versionen des Symantec Management-Agent ausführen. Sie können den Modus "Legacy-Agent-Kommunikation" in der Symantec Management Console auf der Seite "Notification Server-Einstellungen" auf der Registerkarte "Verarbeitung" verwalten.

Siehe "Informationen zur Legacy-Agent-Kommunikation" auf Seite 284.

Siehe "Konfigurieren von Notification Server-Einstellungen" auf Seite 68.

So konfigurieren Sie die Aktualisierungs- und Deinstallationsrichtlinien für den Agent

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster den Ordner "Einstellungen > Agents/Plugins > Symantec Management-Agent" und führen Sie anschließend eine der folgenden Aktionen aus:

So konfigurieren Sie die Aktualisierungsrichtlinie für den Symantec Management-Agent.	■ Erweitern Sie unter Windows x64 den Eintrag "Windows > Non-Site Server" und klicken Sie dann auf "Symantec Management-Agent für Windows x64 (Non-Site Server) - Upgrade auf 64-Bit-Symantec Management-Agent". ■ Erweitern Sie unter Windows x86 den Eintrag "Windows > Non-Site Server" und klicken Sie dann auf "Symantec Management-Agent für Windows x86 (Non-Site Server) - Upgrade auf 32-Bit-Symantec Management-Agent".
So konfigurieren Sie die Richtlinie, die den Symantec Management-Agent auf den Computern aktualisiert, die einen oder mehrere Site Services enthalten	■ Erweitern Sie unter Windows x64 den Eintrag "Windows > Site Server" und klicken Sie dann auf "Symantec Management-Agent für Windows x64 (Nur Site Server) - Upgrade auf 64-Bit-Symantec Management-Agent". ■ Erweitern Sie unter Windows x86 den Eintrag "Windows > Site Server" und klicken Sie dann auf "Symantec Management-Agent für Windows x86 (Nur Site Server) - Upgrade auf 32-Bit-Symantec Management-Agent".
So konfigurieren Sie die Deinstallationsrichtlinie für den Symantec Management-Agent.	Erweitern Sie den Ordner "Windows" und wählen Sie anschließend "Symantec Management-Agent für Windows – Deinstallieren".
So konfigurieren Sie die Aktualisierungsrichtlinie für den Symantec Management-Agent für UNIX/Linux/Mac.	Erweitern Sie den Ordner "UNIX/Linux/Mac" und wählen Sie "Symantec Management-Agent für UNIX/Linux/Mac – Upgrade".
So konfigurieren Sie die Deinstallationsrichtlinie für Symantec Management-Agent für UNIX/Linux/Mac.	Erweitern Sie den Ordner "UNIX/Linux/Mac" und wählen Sie "Symantec Management-Agent für UNIX/Linux/Mac – Deinstallation".

3 Im rechten Teilfenster nehmen Sie die entsprechenden Konfigurationsänderungen vor:

Programmname	Der Name des Symantec Management-Agent-Paketprogramms, das ausgeführt wird, wenn die Richtlinie ausgelöst wurde. Die Standardeinstellung ist das für die Richtlinie geeignete Programm und normalerweise muss diese Einstellung nicht geändert werden. Wenn Sie dem Symantec Management-Agent-Paket jedoch ein neues Programm hinzugefügt haben, können Sie dieses stattdessen verwenden. Siehe "Verwalten von Paketprogrammen" auf Seite 390.
Detaillierte Berichterstattung über Statusereignisse aktivieren	Aktiviert das Senden von Paketstatusereignissen an den Notification Server. Die Einstellungen unter "Notification Server Ereigniserfassung" in den globalen Einstellungen für den Symantec Management-Agent haben Vorrang vor der Einstellung "Detaillierte Berichterstattung über Statusereignisse aktivieren". Ereignisse werden nur gesendet, wenn sie in der Richtlinie "Globale Einstellungen für Symantec Management-Agent" aktiviert sind. Siehe "Konfigurieren der globalen Agent-Einstellungen" auf Seite 290.
Gilt für	Gibt die Computer an, für die die Richtlinie gilt. Sie können die in Notification Server enthaltenen vordefinierten Filter verwenden oder Ihre eigenen Filter erstellen. Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

Paket-Multicast	Deaktiviert das Herunterladen von Paketen über Multicast. Multicast verlangsamt normalerweise den Paket-Rollout. Daher ist es bei einem dringlichen Patch sinnvoll, Multicast auszuschalten. Außerdem funktioniert Multicast in bestimmten Umgebungen nicht. Es könnte beispielsweise auf Routern und Switches deaktiviert sein. Die "Paket-Multicast" -Einstellungen in der Richtlinie "Globale Einstellungen für Symantec Management-Agent" haben Vorrang vor den hier vorgenommenen Einstellungen.
Zeitplan	Der Zeitplan für die Richtlinie. Siehe "Angeben von Richtlinienzeitplänen" auf Seite 404.

4 Aktivieren Sie die Richtlinie.

Klicken Sie oben rechts auf der Seite auf den farbigen Kreis und dann auf "Ein".

5 Klicken Sie auf "Änderungen speichern".

Informationen zur Legacy-Agent-Kommunikation

Im Modus "Legacy-Agent-Kommunikation" können Sie festlegen, ob die Computer, die ältere Versionen des Symantec Management-Agents verwenden, mit dem aktualisierten Notification Server kommunizieren können. Durch diese Option können Sie die Agents in Ihrer Umgebung phasenweise aktualisieren, anstatt sie alle unmittelbar nach dem Upgrade des Notification Servers zu aktualisieren.

Je nachdem, ob der Modus "Legacy-Agent-Kommunikation" aktiviert oder deaktiviert is, kann der Notification Server die Agents wie folgt verwalten:

Der Modus "Legacy-Agent-Kommunikation" ist deaktiviert.	Der Notification Server kann nur die Computer aktiv verwalten, die über die gleiche Version des Symantec Management-Agents wie die Version dieses Notification Servers verfügen. Außerdem kann der Notification Server den Symantec Management-Agent auf den Computern aktualisieren, die zuvor von dem gleichen Notification Server verwaltet wurden.

Der Modus "Legacy-Agent-Kommunikation" ist aktiviert.	Der Notification Server kann bestimmte Verwaltungsfunktionen auf den Computern durchführen, die über eine ältere Version des Symantec Management-Agent als die Version des Notification Server verfügen. **Hinweis:** Wenn der Modus "Legacy-Agent-Kommunikation" aktiviert ist, sehen die Benutzer, die der Rolle "Symantec Administratoren" zugewiesen sind, einen Benachrichtigungs-Banner in der oberen rechten Ecke der Symantec Management Console, sofern sie die Anzeige dieser Benachrichtigung nicht deaktiviert haben.

Bei Symantec Management Agent 7.1 SP1b und höher unterstützt der Modus "Legacy-Agent-Kommunikation" die Verwaltung veralteter Agents mit den folgenden Plugins:

Windows	Software Management, Patch-Management, Inventory und pcAnywhere.
UNIX und Linux	Software Management und Inventory.
Mac OS X	Inventory.

Symantec empfiehlt, dass Sie den Modus "Legacy-Agent-Kommunikation" nach dem Wechsel von der früheren Version von IT Management Suite auf Version 7.5 deaktivieren, damit bei aktiviertem Modus "Legacy-Agent-Kommunikation" der Funktionsumfang des Produkts nicht eingeschränkt ist.

Sie können den Modus "Legacy-Agent-Kommunikation" in der Symantec Management Console auf der Seite "Notification Server-Einstellungen" auf der Registerkarte "Verarbeitung" konfigurieren.

Siehe "Konfigurieren von Notification Server-Einstellungen" auf Seite 68.

Der standardmäßige Modus "Legacy-Agent-Kommunikation" sieht in den folgenden Szenarien wie folgt aus:

- Wenn Sie eine Neuinstallation von IT Management Suite 7.5 durchführen, ist der Modus "Legacy-Agent-Kommunikation" deaktiviert.
- Wenn Sie ein Upgrade von IT Management Suite 7.0 oder 7.1 auf IT Management Suite 7.5 durchführen, ist der Modus "Legacy-Agent-Kommunikation" aktiviert.
- Wenn Sie ein Upgrade von Notification Server 6.x auf IT Management Suite 7.5 durchführen, ist der Modus "Legacy-Agent-Kommunikation" aktiviert.

Konfigurieren des Symantec Management-Agent-Pakets

Die Symantec Management-Agent-Installationsrichtlinien verwenden das entsprechende Symantec Management-Agent-Paket, wenn Sie einen Agent aktualisieren oder deinstallieren. Symantec empfiehlt, keine Änderungen an den Einstellungen dieses Pakets vorzunehmen.

Nachdem Sie ein Symantec Management Agent-Paket konfiguriert haben, müssen Sie die Paketverteilungspunkte aktualisieren, um die Paketinformationen auf jedem Paketserver zu aktualisieren.

Siehe "Aktualisieren der Verteilungspunkte für ein Paket" auf Seite 388.

So konfigurieren Sie ein Symantec Management-Agent-Paket

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster den Ordner "Einstellungen > Agents/Plugins > Symantec Management-Agent".
3. Wählen Sie je nach Konfiguration im Ordner "Windows" bzw. "UNIX/Linux/Mac" das Symantec Management-Agent-Paket aus, das Sie konfigurieren möchten.
4. Ändern Sie auf der Seite "Symantec Management-Agent-Paket" die notwendigen Konfigurationseinstellungen auf den relevanten Registerkarten.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.
5. Klicken Sie auf "Änderungen speichern".

Manuelles Entfernen des Symantec Management-Agent unter Windows

Sie können den Symantec Management-Agent manuell von den ausgewählten Computern entfernen.

So entfernen Sie den Symantec Management-Agent manuell

1. Wählen Sie in der Symantec Management Console im Menü "Aktionen" die Option "Agents/Plugins > Symantec Management-Agent - Push".
2. Wählen Sie auf der Seite "Symantec Management Agent – Installation" die Windows-Computer aus, von denen der Symantec Management-Agent entfernt werden soll.

3 Klicken Sie auf der Seite "Symantec Management-Agent – Installation" unter "Agent-Rollout an Computer" auf "Deinstallation".

4 Aktivieren Sie im Dialogfeld "Symantec Management-Agent – Deinstallationsoptionen" die gewünschten Optionen und geben Sie die notwendigen Einstellungen in den entsprechenden Feldern an.

Proxy verwenden (falls auf dem Zielcomputer konfiguriert)	Verwenden Sie diese Option, wenn der Computer, auf dem eine Push-Installation durchgeführt wird, über einen Proxy-Server eine Verbindung zu Notification Server herstellen muss. Als Proxy-Einstellungen für die Verbindung zu Notification Server werden dieselben Einstellungen verwendet, die Internet Explorer verwendet.
Folgendes Admin-Konto verwenden	Es ist ein Administratorkonto erforderlich, um den Deinstallationsdienst auf dem Computer zu starten, von dem der Symantec Management-Agent deinstalliert wird. Standardmäßig wird die Notification Server-Anwendungsidentität verwendet. Wenn dieses Konto keine Berechtigung für den Zugriff auf den Computer hat, muss ein anderes Konto verwendet werden. Sie müssen den entsprechenden Administratorkonto-Benutzernamen mit zugehörigem Kennwort angeben, der/das verwendet werden soll.

5 Klicken Sie auf "Deinstallation fortsetzen".

Kapitel 17

Konfigurieren des Symantec Management Agent

In diesem Kapitel werden folgende Themen behandelt:

- Konfigurieren des Symantec Management-Agent

Konfigurieren des Symantec Management-Agent

Die Standard-Konfigurationseinstellungen für Symantec-Management-Agent sind für eine kleine Symantec Management-Plattform-Umgebung geeignet. Wenn sich die Größe Ihrer Umgebung ändert oder Ihr Unternehmen besondere Anforderungen stellt, müssen Sie die Konfigurationseinstellungen entsprechend ändern.

Die Agent-Konfigurationseinstellungen werden mithilfe von Agent-Konfigurationseinstellungen auf die relevanten verwalteten Computer übertragen. Sie können diese Richtlinien ändern, um die Einstellungen jederzeit zu ändern. Die neuen Konfigurationseinstellungen werden auf die Agents übertragen, sobald die verwalteten Computer ihre nächsten Richtlinienaktualisierungen erhalten (normalerweise einmal pro Tag).

Tabelle 17-1 Typen von Agent-Konfigurationsrichtlinien

Typ	Beschreibung
Globale Einstellungen	Die globalen Konfigurationseinstellungen gelten für alle Symantec Management-Agents auf allen verwalteten Computern. Diese Einstellungen werden im Rahmen einer einzigen Richtlinie angewendet, die automatisch auf jeden verwalteten Computer übertragen wird. Siehe "Konfigurieren der globalen Agent-Einstellungen" auf Seite 290.

Typ	Beschreibung
Spezifischen Einstellungen	Die spezifischen Agent-Einstellungen sind die allgemeinen Parameter, die den Symantec Management-Agent steuern, u. a. auch die Kommunikation mit dem Notification Server. Die mit der Symantec Management-Plattform gelieferten Standardrichtlinien können geändert werden. Sie können eigene spezifische Einstellungen für Agent-Richtlinien erstellen und auf die gewünschten verwalteten Computer anwenden. Siehe "Konfigurieren der spezifischen Einstellungen" auf Seite 290.
Wartungsfenster	Ein Wartungsfenster ist die vorgesehene Zeitspanne und Dauer, wenn Wartungsvorgänge auf einem verwalteten Computer ausgeführt werden. Eine Wartungsfensterrichtlinie definiert mindestens ein Wartungsfenster. Die mit der Symantec Management-Plattform gelieferte Standardrichtlinie kann von Ihnen geändert werden. Sie können eigene Wartungsfensterrichtlinien erstellen und auf die gewünschten verwalteten Computer übertragen. Siehe "Konfigurieren von Wartungsfensterrichtlinien" auf Seite 292.

Die Richtlinien für spezifische Einstellungen und Wartungsfensterrichtlinien werden auf verwaltete Computer übertragen, die in den angegebenen Richtlinienzielen eingeschlossen sind. Diese Ziele dürfen sich nicht gegenseitig ausschließen. Es dürfen zwei oder mehr Richtlinien desselben Typs für denselben verwalteten Computer gelten.

Wenn auf einen verwalteten Computer zwei oder mehr spezifische Richtlinien übertragen werden, wählt Notification Server die zu verwendende Richtlinie aus. Die Auswahl basiert auf der Richtlinien-GUID und ist für den Benutzer nicht transparent. Sie können nicht vorab bestimmen, welche Richtlinie ausgewählt wird. Sobald die Auswahl getroffen wurde, wird jedoch immer die gleiche Richtlinie verwendet, um sicherzustellen, dass bei jeder Richtlinienaktualisierung dieselbe Richtlinie übertragen wird.

Wenn zwei oder mehr Wartungsfensterrichtlinien für denselben verwalteten Computer gelten, werden die Richtlinien zusammengeführt. Es werden alle angegebenen Wartungsfenster verwendet.

Konfigurieren der globalen Agent-Einstellungen

Die globalen Konfigurationseinstellungen sind diejenigen, für die Sie im Normalfall keine unterschiedlichen Einstellungen auf unterschiedlichen Computern festlegen müssen. Das heißt, sie gelten für alle Symantec Management-Agents auf allen verwalteten Computern. Diese Einstellungen werden als Richtlinie für globale Agent-Einstellungen übertragen. Das bedeutet, dass sie auf die gleiche Weise aktualisiert werden wie andere Richtlinien. Standardmäßig wird die Richtlinie für die globalen Agent-Einstellungen stündlich aktualisiert. Sie können die Richtlinie für die globalen Agent-Einstellungen löschen oder deaktivieren oder alternative Versionen dieser Richtlinie erstellen.

Wenn Sie Agent-Einstellungen für bestimmte Gruppen verwalteter Computer angeben möchten, müssen Sie die erforderlichen Richtlinien für spezifische Agent-Einstellungen konfigurieren.

So konfigurieren Sie die globalen Agent-Einstellungen

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Agents/Plugins" > "Globale Einstellungen".
2. Legen Sie die erforderlichen Konfigurationseinstellungen auf den folgenden Registerkarten fest:

Allgemein	Legen Sie Einstellungen für Tickle/Energieverwaltung und Paket-Multicast fest.
Authentifizierung	Geben Sie Benutzername und Kennwort ein, die Symantec Management-Agent verwendet, um eine Verbindung mit einem Notification Server oder einem Package Server herzustellen.
Ereignisse	Geben Sie Notification Server-Ereignisse an, die Sie aufzeichnen möchten.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.

3. Klicken Sie auf "Änderungen speichern".

Siehe "Konfigurieren des Symantec Management-Agent" auf Seite 288.

Konfigurieren der spezifischen Einstellungen

Mit der Agent-Zieleinstellungsrichtlinie können Sie die allgemeinen Parameter konfigurieren, die den Symantec Management Agent steuern, u. a. auch die Kommunikation mit dem Notification Server. Sie können diese Einstellungen auf bestimmte Computergruppen anwenden. Beispielsweise können einige Computergruppen verschiedene Aufgaben haben oder Sie möchten Server anders

behandeln als andere verwaltete Computer. Sie können die Standardrichtlinien ändern, die mit Notification Server geliefert werden, oder Ihre eigenen Ziel-Agent-Einstellungsrichtlinien erstellen.

Wenn Sie einige Konfigurationseinstellungen angeben möchten, die auf alle Symantec Management-Agents auf allen verwalteten Computern angewendet werden sollen, müssen Sie die globale Agent-Einstellungsrichtlinie konfigurieren.

So konfigurieren Sie die spezifischen Einstellungen

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Agents/Plugins > Spezifische Einstellungen".
2. Führen Sie im linken Bereich einen der folgenden Vorgänge aus:
   - Klicken Sie zum Erstellen einer Richtlinie für spezifische Einstellungen auf "Neu erstellen".
   - Klicken Sie zum Festlegen bzw. Ändern des Richtliniennamens auf die gewünschte Richtlinie und dann auf "Umbenennen".
     Geben Sie im Dialogfeld "Element umbenennen" den neuen Namen ein und klicken Sie dann auf "OK".

3 Nehmen Sie im rechten Teilfenster die erforderlichen Konfigurationseinstellungen auf den folgenden Registerkarten vor:

Allgemein	Zu den allgemeinen Einstellungen gehören die Häufigkeit des Herunterladens von Richtlinie und der Erfassung von Inventardaten sowie die Computer, Benutzer oder Ressourcenziele, auf die die Richtlinie angewendet wird.
UNIX/Linux/Mac	Wenn Symantec Management Agent für UNIX, Linux und Mac installiert wurde, ist diese Registerkarte verfügbar und enthält allgemeine Einstellungen für verwaltete UNIX-, Linux- und MacOS-Computer an.
Downloads	Downloadeinstellungen legen fest, wie jeder Agent Pakete während der Softwareverteilung herunterlädt. Sie können Multicast-Downloads aktivieren und Multicast für Master- und Client-Sitzungen konfigurieren. Sie können diese Einstellungen für einzelne Softwareverteilungsrichtlinien und -aufgaben aufheben.
Sperren	Gesperrte Zeiträume enthalten Zeiten, in denen alle Kommunikation zwischen dem Agent und dem Notification Server deaktiviert wird. Sie können mehrere Sperrzeiträumen einrichten.
Benutzersteuerung	Die Einstellungen für die Benutzersteuerung legen fest, was der Benutzer des verwalteten Computers sehen kann.
Erweitert	Auf dieser Registerkarte können Sie eine alternative URL angeben, über die der Symantec Management Agent auf den Notification Server zugreifen kann, sowie die Energieverwaltungsfunktion aktivieren.

Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.

4 (Optional) Klicken Sie zum Wiederherstellen der Standardeinstellungen für die Richtlinie auf "Standard wiederherstellen".

5 Klicken Sie auf "Änderungen speichern".

Siehe "Konfigurieren des Symantec Management-Agent" auf Seite 288.

Konfigurieren von Wartungsfensterrichtlinien

Ein Wartungsfenster ist die vorgesehene Zeitspanne und Dauer, wenn Wartungsvorgänge auf einem verwalteten Computer ausgeführt werden. Ein Wartungsvorgang ist eine Aktion, die den Status eines Computers ändert, einen

Neustart bewirkt oder die Verwendung des Computers durch den Benutzer beeinträchtigt. Zu den Wartungsvorgängen gehören beispielsweise das Installieren von Software- und Betriebssystem-Patches oder das Ausführen eines Virenscans.

Eine Richtlinie für Wartungsfenster definiert ein oder mehrere Wartungsfenster und wird wie jede andere Richtlinie auf ein Ressourcenziel angewandt. Diese Richtlinien bieten maximale Flexibilität bei der Zuweisung von Wartungsfenstern, ohne die Verwaltung von Agent-Einstellungen zu erschweren. Wenn für einen Computer mehrere Wartungsfenster-Richtlinien gelten, kann der Computer in jedem dieser Wartungsfenster geändert werden.

Mithilfe von Wartungsfenstern können Sie Wartungsarbeiten auf verwalteten Computern mit minimaler Beeinträchtigung des täglichen Betriebs planen. Außerdem können Wartungsvorgänge für unternehmenskritische Server zu unterschiedlichen Zeiten geplant werden, sodass zwei Server nie zum selben Zeitpunkt neu gestartet werden. Wartungsfenster können für einen bestimmten Zeitpunkt geplant werden, z.B. täglich, wöchentlich oder monatlich. Das Wartungsfenster kann zeitlich unbegrenzt eingerichtet werden oder auf eine bestimmte Zeitspanne begrenzt werden.

Wenn Sie ein Wartungsfenster auf einen verwalteten Computer anwenden, können Wartungsaufgaben wie die Verteilung von Patches und Software nur während der geplanten Zeitspanne auf diesem Computer ausgeführt werden. Symantec Management-Agents können jederzeit Software Delivery-Pakete herunterladen, doch können die zugehörigen Programme nur während der Wartungsfenster ausgeführt werden.

Der Symantec Management-Agent verarbeitet die Richtlinie und stellt die Funktionalität zur Verfügung, mit der die Lösungen ermitteln, ob zu dem betreffenden Zeitpunkt ein Wartungsfenster geöffnet ist. Die Funktionalität ermöglicht es den Lösungen auch, Notification Server zu informieren, dass eine Wartungsaufgabe durchgeführt wurde.

Wenn der Symantec Management-Agent als Teil eines Jobs eine Aufgabe ausführt und das Wartungsfenster abläuft, wird das Wartungsfenster automatisch verlängert, damit alle im Job enthaltenen Aufgaben ausgeführt werden können.

Sie können eigene Wartungsfensterrichtlinien erstellen und bearbeiten und auf die gewünschten Ziele übertragen. Die Standardrichtlinie für Wartungsfenster wird auf alle verwalteten Computer übertragen.

So konfigurieren Sie Wartungsfensterrichtlinien.

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Agents/Plugins" > "Wartungsfenster".
2. Führen Sie im linken Teilfenster einen der folgenden Vorgänge aus:

- Klicken Sie zum Erstellen einer neuen Wartungsfensterrichtlinie mit der rechten Maustaste auf den Ordner "Wartungsfenster" und wählen Sie im Kontextmenü die Option "Neu > Wartungsfenster".
- Klicken Sie zum Ändern einer vorhandenen Wartungsfensterrichtlinie auf die entsprechende Richtlinie.

3 Klicken Sie im rechten Teilfenster in der Dropdown-Liste "Zeitzone" auf die gewünschte Option:

Zeit des Agents verwenden	Die Uhrzeit wird ohne Zeitzoneninformationen angegeben und zur lokalen Uhrzeit des jeweiligen verwalteten Computers angewandt. Wartungsfenster werden je nach Zeitzone der verwalteten Computer zu unterschiedlichen Zeiten geöffnet und geschlossen.
Zeit des Servers verwenden	Die Uhrzeit wird mit Zeitzoneninformationen angegeben. Die Zeitzonenanpassung entspricht dabei der Zeitzone des Servers, auf dem die Richtlinie definiert wird. Die Wartungsfenster werden unabhängig von der Zeitzone simultan geöffnet und im Hinblick auf die Sommerzeit angepasst. Diese Option gewährleistet, dass Wartungsfenster stets mit der angegebenen lokalen Uhrzeit des Servers, auf dem die Richtlinie erstellt wird, synchronisiert werden.
Nach UTC koordinieren	Die Uhrzeit wird mit Zeitzoneninformationen angegeben, wobei die Zeitzonenanpassung 0 entspricht. Die Wartungsfenster werden unabhängig von der Zeitzone simultan geöffnet und sind nicht von der Sommerzeit betroffen.

Die Zeitzone gilt für alle Wartungsfenster, die in dieser Richtlinie angegeben werden.

4 Soll die Richtlinie an einem bestimmten Datum in Kraft treten, klicken Sie in der rechten oberen Ecke auf "Erweitert", legen Sie anschließend im Dialogfeld "Erweiterte Optionen" Start- und Enddatum fest und klicken Sie auf "OK".

Start	Das Datum, an dem die Richtlinie in Kraft tritt. Die Richtlinie muss genau wie jede andere Richtlinie aktiviert werden. Sie können die Richtlinie jederzeit vor oder nach dem Startdatum aktivieren.
Ende	Wenn die Richtlinie für einen begrenzten Zeitraum verfügbar sein soll, legen Sie das Enddatum entsprechend fest. Nach diesem Datum steht die Richtlinie dann nicht mehr zur Verfügung, egal ob Sie aktiviert ist oder nicht. Diese Einstellung ist optional. Wenn kein Enddatum festgelegt wird, steht die Richtlinie unbegrenzt zur Verfügung.

5 Klicken Sie zum Erstellen der Wartungsfenster, die in die Richtlinie aufgenommen werden sollen, auf "Wartungsfenster hinzufügen".

6 In den Wartungsfenstern haben Sie folgende Möglichkeiten:

- Geben Sie unter "Tägliche Zeiten" die Startzeit des Wartungsfensters und entweder die Endzeit oder die Dauer in den dafür vorgesehenen Feldern ein.
  Sie können auch den grünen (Startzeit) und roten (Endzeit) Pfeil an die gewünschte Position auf der Zeitleiste ziehen.
- Wählen Sie unter "Wiederholungsplan" in der Dropdown-Liste "Wiederholen alle" einen Zeitplan aus und geben Sie dann die gewünschten Zeitplanfilter an.

7 Geben Sie unter "Gilt für" das Ziel für die Wartungsfensterrichtlinie an.

Sie können eine vorhandene Organisationsgruppe, einen Filter oder ein Ressourcenziel angeben. Sie können jedoch auch individuelle Ressourcen auswählen.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

Details der ausgewählten Elemente werden im Raster angezeigt. Sie können die Liste nach Zielen, Ressourcen, Computer oder Benutzer anzeigen und alle erforderlichen Erweiterungen und Löschungen durchführen.

8 Klicken Sie auf "Änderungen speichern".

Siehe "Konfigurieren des Symantec Management-Agent" auf Seite 288.

Abschnitt 5

Implementieren der Cloud-fähigen Verwaltung

- Kapitel 18. Einführung in die Cloud-fähige Verwaltung
- Kapitel 19. Vorbereiten der Umgebung auf die Cloud-fähige Verwaltung
- Kapitel 20. Einrichten der Cloud-fähigen Verwaltung
- Kapitel 21. Ausführen von Aufgaben in der Cloud-fähigen Verwaltung

Kapitel 18

Einführung in die Cloud-fähige Verwaltung

In diesem Kapitel werden folgende Themen behandelt:

- Info zu Cloud-fähiger Verwaltung

Info zu Cloud-fähiger Verwaltung

Mit der Cloud-fähigen Verwaltung können Sie Endgeräte über das Internet verwalten, selbst, wenn sich die Clientcomputer außerhalb der Unternehmensumgebung befinden und nicht direkt auf die Management-Server zugreifen können. Die verwalteten Computer benötigen keine VPN-Verbindung zu Ihrem Unternehmensnetzwerk.

Sie können die Cloud-fähige Verwaltung in folgenden Szenarien anwenden:

- In Unternehmen, in denen viele Mitarbeiter reisen oder außerhalb des Büros arbeiten (außerhalb des Intranets des Unternehmens).
- Ein MSP (Managed Service Provider), der externe Unternehmen verwaltet.
- Bei hoch verteilten Unternehmen mit vielen kleinen Büros oder Angestellten, die von zu Hause aus arbeiten.

Wenn Sie die Cloud-fähige Verwaltung implementieren, besteht keine direkte Verbindung zwischen Notification Server-Computer, Site Server und dem Internet. Deshalb kommuniziert Symantec Management Agent mit dem Notification Server-Computer und den Site Servern über ein Internet-Gateway. Normalerweise sollten zwei oder mehr Internet-Gateways verfügbar sein, um eine zuverlässige Verwaltung von Cloud-fähigen Clients beizubehalten und Failoveroptionen zur Verfügung zu stellen. Jedes Gateway kann das Weiterleiten an mehrere unabhängige Notification Server unterstützen.

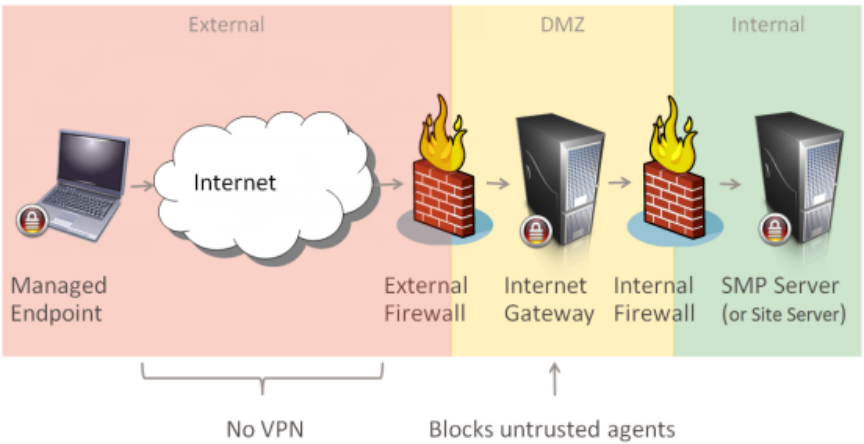
Zur Verwendung der Cloud-fähigen Verwaltung müssen Sie einen Internet-Gatewayserver installieren. Das Internet-Gateway fungiert als Tunnelling-Proxy. Es stellt den Datenschutz und die Sicherheit der Daten sicher, die zwischen einen Agent und einen Management-Server mit HTTPS-Kommunikationen geleitet geworden wird. Das Internet-Gateway befindet sich in einer demilitarisierten Zone (DMZ) zwischen zwei Firewalls. Es akzeptiert eingehende Verbindungen von autorisierten Clientcomputern im Internet und leitet sie an die entsprechenden Notification Server und Site Server innerhalb Ihres Netzwerks weiter. Das Gateway blockiert alle Verbindungsversuche durch nicht autorisierte Clients.

Symantec Management Agent legt automatisch fest, ob es erforderlich ist, die Kommunikation über das Internet-Gateway umzuleiten oder nicht. Wenn ein Cloud-fähiger Computer über das VPN Direktzugriff zum lokalen Netzwerk hat, wechselt der Agent automatisch zu einer direkten Verbindung mit dem Notification Server. Wenn sich ein Cloud-fähiger Computer außerhalb des Unternehmensnetzwerks befindet, leitet der Agent alle Internetverbindungen über das Internet-Gateway auf den Notification Server um.

Hinweis: Die Cloud-fähige Verwaltung wird nur auf Microsoft Windows-Clientcomputern unterstützt.

Die Cloud-fähige Verwaltung ist nur dann auf Ihrer Symantec Management-Plattform verfügbar, wenn eine oder mehrere der installierten Lösungen Cloud-fähige Verwaltung unterstützen. Nicht alle Symantec-Lösungen unterstützen die Cloud-fähige Verwaltung in der IT Management Suite 7.5. Weitere Informationen zur Unterstützung der Cloud-fähigen Verwaltung für eine bestimmte Lösung finden Sie in der Dokumentation der jeweiligen Lösung.

Abbildung 18-1 Cloud-fähige Verwaltung



Um die Cloud-fähige Verwaltung nutzen zu können, müssen Sie die folgenden Aufgaben durchführen:

- Richten Sie die Infrastruktur ein und konfigurieren Sie Ihre Server und Clientcomputer so, dass sie SSL verwenden.
  Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.
- Installieren und konfigurieren Sie die Internet-Gateways, konfigurieren Sie die Richtlinien für die Cloud-fähige Verwaltung und richten Sie die Symantec Management Agents so ein, dass sie die Umgebung der Cloud-fähigen Verwaltung unterstützen.
  Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.
- (Optional) Führen Sie Fehlerbehebungs- und Wartungsaufgaben durch.
  Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Kapitel 19

Vorbereiten der Umgebung auf die Cloud-fähige Verwaltung

In diesem Kapitel werden folgende Themen behandelt:

- Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung

Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung

Das Konfigurieren Ihrer Umgebung zur Verwendung von SSL ist eine Voraussetzung für das Einrichten der Cloud-fähigen Verwaltung. Nachdem Sie Ihre Umgebung zur Verwendung von SSL konfiguriert haben, können Sie mit der Einrichtung der Cloud-fähigen Verwaltung beginnen.

Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

Tabelle 19-1 Prozess zur Vorbereitung Ihrer Umgebung auf die Cloud-fähige Verwaltung

Schritt	Aktion	Beschreibung
Schritt 1	Konfigurieren Sie Ihre Notification Server- und Symantec Management-Agents zur Verwendung von HTTPS.	Zuerst müssen Sie sicherstellen, ob Ihre Notification Server für HTTPS-Zugriff konfiguriert werden und dass Ihre Symantec Management-Agents HTTPS verwenden. Notification Server wird automatisch zur Verwendung von HTTPS konfiguriert, wenn Sie während der Installation der IT Management Suite das Kontrollkästchen "HTTPS zum Zugreifen auf die Management-Plattform erforderlich" auf der Seite "Notification Server-Konfiguration" im Symantec Installation Manager aktivieren. Wenn Sie Symantec Management-Agents von einem Notification Server verteilen, der HTTPS verwendet, werden die Symantec Management-Agents auch automatisch so konfiguriert, dass sie HTTPS verwenden. Wenn Sie Notification Server ohne Unterstützung installieren, können Sie ihn manuell später konfigurieren. Außerdem müssen Sie die Symantec Management-Agents umleiten, damit sie HTTPS für die Kommunikation mit dem Notification Server verwenden. Siehe "Konfigurieren des Notification Servers für die Verwendung von HTTPS" auf Seite 304. Siehe "Anwenden eines Zertifikats einer Stammzertifizierungsstelle auf einen verwalteten Computer" auf Seite 305. Siehe "Umleiten eines Symantec Management-Agent für die Verwendung von HTTPS" auf Seite 308.

Schritt	Aktion	Beschreibung
Schritt 2	Bereiten Sie Ihre Site Server-Computer vor.	Cloud-fähige Clientcomputer müssen die Identität des Site Servers überprüfen. Dafür können Sie ein kommerzielles Zertifikat oder Ihre eigene Public Key-Infrastruktur (PKI) verwenden oder der Notification Server fungiert als Zertifzierungsstelle (CA) und generiert Zertifikate für Ihre Site Server. Cloud-fähige Verwaltung weist Site Servern keine Serverzertifikate zu. Sie müssen Serverzertifikate auf Site Server anwenden, damit diese über HTTPS zugänglich sind. Ein Serverzertifikat ist eine Voraussetzung für alle Site Server, die Symantec Management-Agents über das Internet verarbeiten. Mit dem Tool zum Generieren des Site Server-Zertifikats (`AeXGenSiteServerCert.exe`) können Sie ein Serverzertifikat erstellen. Der Zertifikatname muss dem Namen des Site Servers entsprechen. Auch dieses Zertifikat wird durch das spezielle Notification Server-Zertifikat der Zertifizierungsstelle für (CA) Cloud-fähige Clients gekennzeichnet. Wenn Sie nicht über eine unternehmenseigene Zertifizierungsstelle verfügen, können Sie mit diesem Tool HTTPS auf Ihren Site Servern leicht einrichten. Um sicherzustellen, ob der Agent auf dem Site Server mit Notification Server unter Verwendung von HTTPS kommunizieren kann, müssen Sie die Zertifizierungsstelle für das Stammzertifikat auf den Site Server-Computer auch anwenden. Siehe "Generieren und Anwenden des Site Server-Zertifikats für Zugriff des Cloud-fähigen Agent" auf Seite 309. Siehe "Anwenden eines Zertifikats einer Stammzertifizierungsstelle auf einen verwalteten Computer" auf Seite 305.
Schritt 3	Führen Sie für Site Services ein Rollout aus.	Nachdem Sie die Site Server-Computer vorbereitet haben, können Sie für die Site Services ein Rollout ausführen. **Hinweis:** Das Ausführen eines Task Servers auf einem Cloud-fähigen, Internet-verwalteten Clientcomputer wird nicht unterstützt und kann zu unerwünschtem Verhalten führen. Siehe "Verwalten von Site Servers" auf Seite 137.

Schritt	Aktion	Beschreibung
Schritt 4	Konfigurieren Sie Package Server so, dass sie HTTPS-Paket-Codebasen veröffentlichen.	Sie müssen sicherstellen, dass Ihre Cloud-fähigen Agents oder Package Server Pakte vom Notification Server oder den internen Package Servern erhalten können. Um ihnen das Herunterladen von Paketen zu ermöglichen, müssen Notification Server und die internen Package Server HTTPS-Paket-Codebasen veröffentlichen. Siehe "Konfigurieren eines Package Servers zur Veröffentlichung von HTTPS-Paket-Codebasen" auf Seite 315. Siehe "Unterstützte Konfigurationen für Package Server in einer gemischten Umgebung" auf Seite 539. **Hinweis:** Package Server veröffentlichen Codebasen mithilfe des FQDN. Wenn Sie ein kommerzielles SSL-Zertifikat verwenden, das der Symantec Management-Plattform zugewiesen ist, können Verbindungsprobleme auftreten. Informationen zur Umgehung dieses Problems finden Sie in folgendem Artikel: TECH210809.
Schritt 5	Konfigurieren Sie Sites und Site Server zur Verarbeitung von internetbasierten Agents.	Die Cloud-fähigen Agents, die sich hinter den Internet-Gateways befinden, verwenden Internetsites zum Festlegen von Site Services. In der Symantec Management Console müssen Sie Ihre Site Server einer vordefinierten "Standard-Internetsite" oder anderen Internetsites hinzufügen, die Sie verwenden möchten. Sie müssen die Cloud-fähigen Computer auch den Sites zuweisen, die auf Ressourcenzielen basieren. Diese manuelle Zuweisung stellt sicher, dass jeder Computer ein Mitglied der entsprechenden Site bleibt, unabhängig davon, ob er sich auch physisch dort befindet. Siehe "Konfigurieren von Sites und Site Servern zum Verarbeiten von Cloud-fähigen Agents" auf Seite 317.
Schritt 6	Stellen Sie sicher, dass die Internetsite richtig konfiguriert ist.	Stellen Sie auf der Seite "Internetsites" sicher, dass die erforderlichen Site Services richtig eingerichtet werden und dass die Einstellungen auf das entsprechende Ressourcenziel angewendet werden. Sie können auf die Seite "Internetsites" in der Symantec Management Console, über die Seite "Site Server-Einstellungen" unter "Site-Verwaltung > Internetsites" zugreifen.

Konfigurieren des Notification Servers für die Verwendung von HTTPS

Wenn Sie Ihren Notification Server während der Installation der IT Management Suite nicht für HTTPS konfigurieren, müssen Sie es manuell tun.

Diese Aufgabe ist ein Schritt beim Vorbereiten Ihrer Umgebung für Cloud-fähige Verwaltung.

Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.

So konfigurieren Sie den Notification Server für die Verwendung von HTTPS

1. Starten Sie Internet Information Services (IIS) Manager auf dem Notification Server-Computer.
2. Bearbeiten Sie die Eigenschaften für die Altiris-Website.

   Führen Sie die Schritte aus, die dem Betriebssystem des Notification Server-Computers entsprechen:

Windows 2003	1. Klicken Sie im Altiris-Fenster "Eigenschaften" auf der Registerkarte "Verzeichnissicherheit" unter "Sichere Kommunikation" auf "Bearbeiten". 2. Aktivieren Sie im Fenster "Sichere Kommunikation" das Kontrollkästchen "Sicheren Kanal voraussetzen (SSL)" und klicken Sie dann auf "OK".
Windows 2008	1. Klicken Sie im mittleren Teilfenster unter "IIS" auf "SSL-Einstellungen". 2. Wählen Sie "SSL erforderlich". 3. Klicken Sie im Teilfenster "Aktionen" auf "Übernehmen".

3. Wenn der Notification Server nicht das Veröffentlichen von HTTPS-Codebasen beginnt, führen Sie folgende Schritte durch:
   - Starten Sie auf dem Notification Server IIS neu.
   - Starten Sie auf dem Notification Server den Altiris-Dienst neu.
   - Führen Sie auf dem Notification Server unter den geplanten Windows-Aufgaben den Zeitplan für die Paketaktualisierung aus.

Um diesen Schritt abzuschließen, müssen Sie außerdem Folgendes ausführen:

Siehe "Anwenden eines Zertifikats einer Stammzertifizierungsstelle auf einen verwalteten Computer" auf Seite 305.

Siehe "Umleiten eines Symantec Management-Agent für die Verwendung von HTTPS" auf Seite 308.

Anwenden eines Zertifikats einer Stammzertifizierungsstelle auf einen verwalteten Computer

Bevor Sie einen verwalteten Computer auf Cloud-fähige Verwaltung migrieren, müssen Sie sicherstellen, dass der Agent über HTTPS mit dem Notification Server und den Site Servern kommunizieren kann. Damit HTTPS für die Kommunikation verwendet werden kann, muss der Agent den Notification Server und die Site Server als vertrauenswürdig einstufen. Bei Bedarf können Sie dem Speicher "Vertrauenswürdige Stammzertifizierungsstellen" des Kontos "Lokaler Computer" auf dem verwalteten Computer die entsprechenden Zertifikate der Zertifierungsstelle für das Stammzertifikat hinzufügen.

Sie können das entsprechende selbstsignierte Zertifikat vom Notification Server exportieren. Wenn der Notification Server kein selbstsigniertes Zertifikat verwendet, müssen Sie die Zertifierungsstelle für das Stammzertifikat für die vom Notification Server verwendete Zertifikatskette exportieren.

Um das exportierte CA-Zertifikat auf einen Clientcomputer anzuwenden, können Sie eine Kommandozeile oder oder die Microsoft Management Console verwenden. Alternativ können Sie die Active Directory-Gruppenrichtlinie für ein Rollout des Zertifikats zu verwenden oder Symantec Management Agent erneut mit aktivierter automatischer Zertifikatbereitstellung installieren.

Diese Aufgabe ist ein Schritt im Prozess für das Vorbereiten Ihrer Umgebung auf die Cloud-fähige Verwaltung.

Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.

Um diesen Schritt abzuschließen, müssen Sie außerdem Folgendes ausführen:

Siehe "Konfigurieren des Notification Servers für die Verwendung von HTTPS" auf Seite 304.

Siehe "Umleiten eines Symantec Management-Agent für die Verwendung von HTTPS" auf Seite 308.

So exportieren Sie ein Stammzertifizierungsstellenzertifikats vom Notification Server

1. Starten Sie auf dem Site Server-Computer die Microsoft Management Console.
2. Fügen Sie das "Zertifikat-Snap-In" für "Computerkonto > Lokaler Computer" hinzu und navigieren Sie dann zu "Konsolenstamm > Zertifikate (lokaler Computer) > Vertrauenswürdige Root-Zertifizierungsstellen > Zertifikate".

3 Klicken Sie mit der rechten Maustaste auf die Zertifizierungsstelle, die Sie exportieren möchten:

SMP <NS_Name>-Agent-Zertifizierungs-stelle	Diese Zertifizierungsstelle stellt Agent-Zertifikate aus. Symantec Management-Agents verwenden diese Zertifikate, wenn sie über ein Internet-Gateway mit dem Notification Server und den Site Servern kommunizieren. Das Internet-Gateway muss diese Zertifizierungsstelle installiert haben, um die betreffenden Clients als vertrauenswürdig einzustufen.
SMP <NS_Name>-Server-Zertifizierungs-stelle	Diese Zertifizierungsstelle stellt Server-Zertifikate aus. Site Server verwenden diese Zertifikate, um sich zu authentifizieren. Wenn Symantec Management-Agents den Site Server kontaktieren, überprüfen sie das Serverzertifikat.

4 Klicken Sie auf "Alle Aufgaben" > "Exportieren".

5 Geben Sie im Zertifikatexport-Assistenten die folgenden Einstellungen an:

- Wählen Sie "Nein, privaten Schlüssel nicht exportieren".
- Wählen Sie "DER-codiert-binär X.509 (.CER)".
- Geben Sie den Pfad und den Namen der exportierten Zertifikatsdatei an.

6 Klicken Sie auf "Fertig stellen" und schließen Sie dann das Popup zur Exportbestätigung.

Anschließend können Sie die Datei zu einem verwalteten Computer bringen und das Zertifikat manuell anwenden. Alternativ können Sie das Zertifikat mithilfe einer Paketverteilungsaufgabe oder einer Active Directory-Gruppenrichtlinie auf den verwalteten Computern verteilen.

So wenden Sie ein Stammzertifizierungsstellenzertifikat manuell mit einer Kommandozeile auf einen verwalteten Computer an

1. Legen Sie auf dem entsprechenden verwalteten Computer die Zertifikatsdatei im Installationsordner des Symantec Management-Agent ab.

   Der Standardordner ist der Ordner *"C:\\Programme*\Altiris\Altiris Agent".

2. Öffnen Sie ein Befehlsfenster und geben Sie die folgende Kommandozeile ein:

   ```
   [Agent-Installationsordner]\AeXNSAgent.exe
   /rootca=Zertifikatsdatei.cer
   ```

   Dieser Befehl fügt das angegebene Zertifikat in den Zertifikatspeicher "Vertrauenswürdige Stammzertifizierungsstellen" ein.

   Beispiel:

   C:\\Programme\Altiris\Altiris Agent\AeXNSAgent.exe /rootca=myClientCert.cer

So wenden Sie ein Stammzertifizierungsstellenzertifikat manuell mit einer Microsoft Management Console auf einen verwalteten Computer an

1. Legen Sie die Zertifikatsdatei an einem Speicherort ab, der vom verwalteten Computer aus zugänglich ist.
2. Starten Sie auf dem verwalteten Computer die Microsoft Management Console.
3. Fügen Sie das "Zertifikat-Snap-In" für das Konto "Lokaler Computer" hinzu und öffnen Sie dann den Ordner "Konsolenstamm > Zertifikate (lokaler Computer)".
4. Klicken Sie mit der rechten Maustaste auf "Vertrauenswürdige Stammzertifizierungsstellen" und wählen Sie dann "Alle Aufgaben" > "Importieren" aus.
5. Geben Sie im Zertifikatimport-Assistenten den Pfad und den Dateinamen der Zertifikatsdatei an, die Sie importieren möchten.
6. Klicken Sie auf "Weiter", um den Standardspeicherort und andere Einstellungen zu akzeptieren, und klicken Sie dann auf "Fertig stellen".

So wenden Sie ein Stammzertifizierungsstellenzertifikat manuell auf einen verwalteten Computer an, indem Sie den Symantec Management-Agent neu installieren

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Expandieren Sie im linken Teilfenster "Agents/Plugins > Symantec Management Agent > Einstellungen" und klicken Sie dann auf "Symantec Management-Agent - Installation".

3 Klicken Sie auf der Seite "Symantec Management-Agent - Installation" auf der Registerkarte "Agent installieren" unter "Agent-Rollout an Computer" auf "Einstellungen".

4 Aktivieren Sie im Dialogfeld "Symantec Management-Agent - Installationsoptionen" die Option "Serverzertifikat auf dem Client-Rechner installieren" und klicken Sie auf "OK".

5 Wählen Sie auf der Seite "Symantec Management-Agent - Installation" auf der Registerkarte "Agent installieren" unter "Agent-Rollout an Computer" die Computer aus, auf denen Symantec Management Agent installiert werden soll und klicken Sie dann auf "Installieren".

Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Umleiten eines Symantec Management-Agent für die Verwendung von HTTPS

Bevor Sie den Symantec Management-Agent unter Cloud-fähige Verwaltung bringen können, müssen Sie sicherstellen, dass der Agent HTTPS für die Kommunikation mit dem Notification Server verwendet. Mit der Richtlinie "Spezifische Einstellungen" können Sie den Agent umleiten, dass er HTTPS verwendet.

Symantec empfiehlt, dass Sie eine benutzerdefinierte spezifische Richtlinie für Cloud-fähige Clients erstellen und diese Clients von anderen spezifischen Richtlinien ausschließen.

Siehe "Konfigurieren der spezifischen Einstellungen" auf Seite 290.

Warnung: Sie müssen sicherstellen, dass der Agent dem SSL-Serverzertifikat vertraut, das der Notification Server für die HTTPS-Kommunikation verwendet. Um das entsprechende Zertifikat auf einen Clientcomputer anzuwenden, können Sie eine Kommandozeile oder Microsoft Management Console verwenden. Außerdem können Sie den Symantec Management-Agent mit aktivierter automatischer Zertifikatbereitstellung neu installieren

Siehe "Anwenden eines Zertifikats einer Stammzertifizierungsstelle auf einen verwalteten Computer" auf Seite 305.

Diese Aufgabe ist ein Schritt im Prozess für das Vorbereiten Ihrer Umgebung auf die Cloud-fähige Verwaltung.

Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.

Um diesen Schritt abzuschließen, müssen Sie außerdem Folgendes ausführen:

Siehe "Konfigurieren des Notification Servers für die Verwendung von HTTPS" auf Seite 304.

Siehe "Anwenden eines Zertifikats einer Stammzertifizierungsstelle auf einen verwalteten Computer" auf Seite 305.

So leiten Sie einen Symantec Management-Agent für die Verwendung von HTTPS um

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Agents/Plugins > Spezifische Einstellungen".
2. Wählen Sie im linken Teilfenster die Richtlinie aus, die für den Computer gilt, den Sie unter die Cloud-fähige Verwaltung stellen möchten.
3. Aktivieren Sie im rechten Teilfenster auf der Registerkarte "Erweitert" unter "Alternative URL für Zugriff auf NS" das entsprechende Kontrollkästchen.
4. Geben Sie die entsprechende HTTPS-URL an, über die der Symantec Management-Agent auf den Notification Server zugreifen kann:

Servername	Der Name des Notification Server-Computers.
Server-Webadresse	Die Webadresse des Notification Servers. Die Adresse muss im folgenden Format vorliegen: **https://*NS_FQDN*[:*port*]/Altiris/**

5. Klicken Sie auf "Änderungen speichern".

   Wenn die Richtlinie auf dem verwalteten Computer aktualisiert wird, leitet sie den Agent so um, dass er HTTPS für die Kommunikation mit dem Notification Server verwendet.

Im nächsten Schritt müssen Sie Ihre Site Server-Computer vorbereiten.

Siehe "Generieren und Anwenden des Site Server-Zertifikats für Zugriff des Cloud-fähigen Agent" auf Seite 309.

Eine detaillierte Beschreibung des Prozesses zum Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung finden Sie unter Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.

Generieren und Anwenden des Site Server-Zertifikats für Zugriff des Cloud-fähigen Agent

Bevor Sie diesen Schritt ausführen, vergewissern Sie sich, dass Sie Ihren Notification Server und die Symantec Management-Agent für die Verwendung von HTTPS konfiguriert haben.

Siehe "Konfigurieren des Notification Servers für die Verwendung von HTTPS" auf Seite 304.

Siehe "Umleiten eines Symantec Management-Agent für die Verwendung von HTTPS" auf Seite 308.

Cloud-fähige Verwaltung weist Site Servern keine Serverzertifikate zu. Sie müssen Serverzertifikate auf Site Server anwenden, damit diese über HTTPS zugänglich sind. Ein Serverzertifikat ist eine Voraussetzung dafür, dass ein Site Server Symantec Management-Agents im Internet bearbeiten kann. Aus Sicherheitsgründen empfiehlt Symantec die Verwendung selbstsignierter Zertifikate.

Sie sollten Ihre eigene Unternehmenszertifizierungsstelle (CA) das Erstellen der erforderlichen Serverzertifikate verwenden, um HTTPS auf Ihren Site Servern einzurichten. Wenn Sie jedoch keine eigene Unternehmenszertifizierungsstelle haben, stellt Symantec Management-Plattform ein Kommandozeilen-Tool bereit, mit dem Sie Serverzertifikate generieren können.

Mithilfe des Tools zum Generieren von Site Server-Zertifikaten, `AeXGenSiteServerCert.exe`, können Sie die erforderlichen Serverzertifikate erstellen. Eine spezielle Serverzertifizierungsstelle auf dem Notification Server stellt das Serverzertifikat aus. Der öffentliche Teil des Zertifikats wird in der Configuration Management Database gespeichert (CMDB). Sowohl der öffentliche als auch der private Teil werden zu einer PKCS#12 (PFX)-Datei hinzugefügt, die die gesamte Zertifikatskette enthält.

Hinweis: Das Tool `AeXGenSiteServerCert.exe` unterstützt nur IIS.

Nachdem Sie die Serverzertifikatsdatei generiert haben, müssen Sie das Zertifikat auf dem entsprechenden Site Server installieren. Das Installationsverfahren hängt davon ab, ob das Serverzertifikat kennwortgeschützt ist oder nicht. Es hängt auch vom Betriebssystem des Site Server-Computers ab.

Beachten Sie, dass bei den Task Server-Computern die Funktionen "IIS 6.0" oder "IIS 7.0" und ".NET Framework 3.5" aktiviert sein müssen.

Hinweis: Das Anwenden eines neu generierten Serverzertifikats auf ein Internet-Gateway hat Auswirkungen auf vorhandene Symantec Management-Agents. Die vorhandenen Agents können erst dann eine Verbindung zum Internet-Gateway herstellen, wenn sie aktualisierte Daten des Fingerabdrucks für das Zertifikat des Gateways erhalten haben. Wenn kein alternatives Internet-Gateway verfügbar ist, können die betroffenen Symantec Management-Agents möglicherweise keine Verbindung zum internen Netzwerk herstellen. Sie müssten die Agent-Konfiguration manuell aktualisieren.

Diese Aufgabe ist ein Schritt im Prozess für das Vorbereiten Ihrer Umgebung auf die Cloud-fähige Verwaltung.

Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.

So generieren Sie ein Serverzertifikat für einen Site Server

1 Öffnen Sie auf dem Notification Server-Computer ein Befehlsfenster und wechseln Sie zum folgenden Verzeichnis:

```
C:\\Programme\Altiris\Notification Server\bin\Tools
```

2 Geben Sie die folgende Kommandozeile mit den entsprechenden Parametern ein:

```
AeXGenSiteServerCert.exe <SiteServerFQDN> [-o
Zertifikatskette.pfx] [-p Kennwort]
```

SiteServerFQDN	Der vom Symantec Management-Agent verwendete Name bei der Herstellung einer Verbindung zum Site Server. Dieser Name ist gewöhnlich der voll qualifizierte Domänenname (FQDN) des Site Server-Computers. Ihr Site Server heißt beispielsweise **"myhost.mydomain.com"**. Der Name auf dem Zertifikat muss dem Namen oder der IP-Adresse entsprechen, die der Agent verwendet, wenn er eine Verbindung zum Site Server herstellt. Wenn der Name bzw. die Adresse nicht übereinstimmt, kann der Agent keine Verbindung zum Site Server herstellen.
Zertifikatskette.pfx	Der Name der PFX-Datei, die Sie generieren möchten. Wenn Sie diesen Parameter auslassen, ist der generierte Zertifikatsdateiname der angegebene allgemeine Name mit der Erweiterung ".pfx" (***AllgemeinerName*.pfx**).
Kennwort	Das Kennwort, das Sie verwenden möchten. Wenn Sie diesen Parameter auslassen, ist das Kennwort leer. Es wird kein Standardkennwort bereitgestellt. IIS-Manager erwartet beim Import eine kennwortgeschützte PFX-Datei. Wenn Ihre PFX-Datei kein Kennwort hat, müssen Sie die Datei zuerst mithilfe von Microsoft Management Console (MMC) in den Site Server-Computer importieren. Anschließend können Sie mithilfe von IIS-Manager das Zertifikat anwenden, indem Sie ein vorhandenes Zertifikat zuweisen.

Die Serverzertifikatdatei wird im gleichen Verzeichnis erstellt, in dem Sie den Befehl ausführen.

So wenden Sie ein Serverzertifikat auf einen Windows 2008-Site Server an

1. Legen Sie die PFX-Datei des Serverzertifikats auf dem Site Server-Computer oder an einem zugänglichen Speicherort ab.
2. Starten Sie auf dem Site Server-Computer den Internet Information Services (IIS)-Manager und klicken Sie im linken Bereich auf *"Computername"*.
3. Doppelklicken Sie im mittleren Teilfenster auf "Serverzertifikate" und klicken Sie dann im Teilfenster "Aktionen" auf "Importieren".
4. Geben Sie im Dialogfeld "Zertifikat importieren" den Pfad und die Datei des Zertifikats, das Sie importieren möchten, an, geben Sie gegebenenfalls das Kennwort ein und klicken Sie auf "OK" an.
5. Klicken Sie im linken Bereich des Internet Information Services (IIS)-Manager unter *"Computername* > Sites" auf "Standard-Website".
6. Klicken Sie im Teilfenster "Aktionen" auf "Bindungen".
7. Führen Sie in der Liste der Bindungen eine der folgenden Aktionen aus:

Stellen Sie eine neue Bindung her.	Klicken Sie auf "Hinzufügen" und legen Sie dann den Typ auf "HTTPS" fest.
Bearbeiten Sie eine vorhandene HTTPS-Bindung	Wählen Sie die Bindung und klicken Sie dann auf "Bearbeiten".

8. Geben Sie im Dialogfeld "Sitebindung hinzufügen" oder "Sitebindung bearbeiten" die zu verwendende Port-Nummer, die abzuhörenden Netzwerkschnittstellen und das zu verwendende SSL-Zertifikat an und klicken Sie dann auf "OK".

   Es wird erwartet, dass sich das Zertifikat im persönlichen Speicher des Kontos "Lokaler Computer" befindet.
9. Starten Sie auf dem Site Server-Computer das "IIS" und die "Altiris Object Host Services" neu.

So wenden Sie ein kennwortgeschütztes Serverzertifikat auf einen Windows 2003-Site Server an

1. Legen Sie die PFX-Datei des Serverzertifikats auf dem Site Server-Computer oder an einem zugänglichen Speicherort ab.
2. Starten Sie auf dem Site Server-Computer IIS-Manager, klicken Sie im linken Teilfenster unter *"Computername* > Websites" mit der rechten Maustaste auf "Standardwebsite" und klicken Sie anschließend auf "Eigenschaften".

3. Klicken Sie im Fenster „Standard-Website - Eigenschaften" auf der Registerkarte "Verzeichnissicherheit" auf "Serverzertifikat".
4. Führen Sie im "IIS-Zertifikat-Assistent" folgende Schritte durch:
   - Klicken Sie auf der Seite "Serverzertifikat" auf "Zertifikat von PFX-Datei importieren" und anschließend auf "Weiter".
   - Geben Sie auf der Seite "Zertifikat importieren" den Pfad und den Dateinamen der Zertifikatsdatei an und klicken Sie auf "Weiter".
   - Geben Sie auf der Seite "Kennwort für zu importierendes Zertifikat" das Kennwort für das Zertifikat ein, das Sie importieren möchten.
   - Geben Sie auf der Seite "SSL-Port" die zu verwendende Port-Nummer an und klicken Sie auf "Weiter".
   - Überprüfen Sie auf der Seite "Importierte Zertifikate - Übersicht" die Zertifikatsdaten und klicken Sie auf "Weiter".
   - Klicken Sie auf "Fertig stellen".
5. Klicken Sie auf "OK", um das Fenster "Standard-Website - Eigenschaften" zu schließen.
6. Starten Sie auf dem Site Server-Computer "IIS" und "Altiris Object Host Services" neu.

So wenden Sie ein Serverzertifikat ohne Kennwort auf einen Windows 2003-Site Server an

1. Starten Sie auf dem Site Server-Computer die Microsoft Management Console.
2. Fügen Sie das "Zertifikat-Snap-In" für das Konto "Lokaler Computer" hinzu und öffnen Sie dann den Ordner "Konsolenstamm > Zertifikate > Privat".
3. Klicken mit der rechten Maustaste auf "Zertifikate" und klicken Sie anschließend auf "Alle Aufgaben > Importieren".
4. Geben Sie im Zertifikatimport-Assistenten die Serverzertifikatdatei an, die Sie importieren möchten.
5. Klicken Sie auf "Weiter", um die Standardeinstellungen für alle verbleibenden Seiten des Zertifikatimport-Assistenten zu akzeptieren, und klicken Sie dann auf "Fertig stellen".

   Das Zertifikat wird zum persönlichen Zertifikatspeicher hinzugefügt.
6. Starten Sie den Internet Information Services (IIS)-Manager und klicken Sie im linken Bereich unter *"Computername* > Websites" mit der rechten Maustaste auf "Standard-Website" und anschließend auf "Eigenschaften".

7. Klicken Sie im Fenster "Eigenschaften" auf der Registerkarte "Verzeichnissicherheit" auf "Serverzertifikat".
8. Klicken Sie im "Assistenten für Webserverzertifikate" auf der Seite "Serverzertifikat" auf "Vorhandenes Zertifikat zuweisen" und anschließend auf "Weiter".
9. Wählen Sie das Zertifikat aus, das Sie importiert haben, und klicken Sie dann auf "Weiter", um die Standardeinstellungen für alle restlichen Seiten zu akzeptieren.
10. Klicken Sie auf "Fertig stellen" und anschließend auf "OK", um das Fenster "Standart-Website - Eigenschaften" zu schließen.

So wenden Sie ein Serverzertifikat auf einen Windows XP-Site Server an

1. Legen Sie die PFX-Datei des Serverzertifikats auf dem Site Server-Computer oder an einem zugänglichen Speicherort ab.
2. Starten Sie auf dem Site Server-Computer die Microsoft Management Console.
3. Fügen Sie das "Zertifikat-Snap-In" für das Konto "Lokaler Computer" hinzu und öffnen Sie dann den Ordner "Konsolenstamm > Zertifikate > Privat".
4. Klicken mit der rechten Maustaste auf "Zertifikate" und klicken Sie anschließend auf "Alle Aufgaben > Importieren".
5. Geben Sie im "Zertifikatimport-Assistent" den Namen und den Pfad der zu importierenden Zertifikatdatei, das Kennwort und den Zertifikatsspeicher an, prüfen Sie die Einstellungen und klicken Sie dann auf "Fertig stellen" an.
6. Klicken Sie im Internet Information Services (IIS)-Manager im linken Bereich unter *"Computername* > Websites" mit der rechten Maustaste auf "Standard-Website" und anschließend auf "Eigenschaften".

   Beachten Sie, dass die Funktionen "IIS 6.0" oder "IIS 7.0" und ".NET Framework 3.5" aktiviert sein müssen.
7. Klicken Sie im Fenster "Standart-Website - Eigenschaften" auf der Registerkarte "Verzeichnissicherheit" auf "Serverzertifikat".
8. Führen Sie im "IIS-Zertifikat-Assistent" folgende Schritte durch:
   - Klicken Sie auf der Seite "Serverzertifikat" auf "Vorhandenes Zertifikat zuweisen" und klicken Sie auf "Weiter".
   - Klicken Sie auf der Seite "Verfügbare Zertifikate" auf die Zertifikatdatei und klicken Sie auf "Weiter".
   - Geben Sie auf der Seite "SSL-Port" die zu verwendende Port-Nummer an und klicken Sie auf "Weiter".

- Überprüfen Sie auf der Seite "Zertifikatübersicht" die Zertifikatdaten und klicken Sie auf "Weiter".
- Klicken Sie auf "Fertig stellen".

9 Klicken Sie auf "OK", um das Fenster "Standard-Website - Eigenschaften" zu schließen.

10 Starten Sie auf dem Site Server-Computer "IIS" und "Altiris Object Host Services" neu.

Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Im nächsten Schritt müssen Sie für Site Services ein Rollout ausführen.

Siehe "Verwalten von Site Servers" auf Seite 137.

Eine detaillierte Beschreibung des Prozesses zum Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung finden Sie unter Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.

Konfigurieren eines Package Servers zur Veröffentlichung von HTTPS-Paket-Codebasen

Stellen Sie sicher, dass Sie für die Site Services ein Rollout ausgeführt haben, bevor Sie diesen Schritt ausführen.

Siehe "Verwalten von Site Servers" auf Seite 137.

Sie können HTTPS auf Ihren Package Servern konfigurieren, indem Sie die Seite "Package Service-Einstellungen" verwenden. Auf dieser Seite werden die globalen Package Service-Einstellungen festgelegt, die auf alle Package Server angewendet werden, die Ihre Symantec Management-Plattform bearbeiten.

Jeden Package Server-Computer muss seine IIS so konfiguriert haben, dass HTTPS-Verbindungen akzeptiert werden. Sie können Ihre interne Unternehmenszertifizierungsstelle verwenden, um die entsprechenden Zertifikate zur Verfügung zu stellen. Wenn Sie keine interne Unternehmenszertifizierungsstelle haben, können Sie ein Notification Server-Kommandozeilenprogramm verwenden, um die erforderlichen Zertifikate für die HTTPS-Konfiguration zu generieren.

Siehe "Generieren und Anwenden des Site Server-Zertifikats für Zugriff des Cloud-fähigen Agent" auf Seite 309.

Sie müssen sicherstellen, dass Ihre Cloud-fähigen Package Server als Downloadquelle für Pakete dienen können. Cloud-fähige Agents und Package Server dürfen Pakete nur mit HTTPS über das Internet-Gateway herunterladen. Um nicht verbundenen Package Servern das Herunterladen von Paketen zu ermöglichen, müssen sowohl der Notification Server als auch die Package Server

derselben Site Codebasen für HTTPS-Pakete veröffentlichen. Diese Konfiguration ist erforderlich, weil ein Package Server, der keine verfügbaren Paketquellen innerhalb seiner eigenen Site hat, Pakete von anderen Sites anfordern muss. Zuerst versucht der Package Server, Pakete von den Package Servern zu beziehen, die sich in derselben Site befinden wie der Notification Server. Wenn keine Package Server verfügbar sind, versucht er, Pakete vom Notification Server selbst zu beziehen.

Diese Aufgabe ist ein Schritt im Prozess für das Vorbereiten Ihrer Umgebung auf die Cloud-fähige Verwaltung.

Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.

So konfigurieren Sie einen Package Server zur Veröffentlichung von HTTPS-Paket-Codebasen

1. Um HTTPS global auf allen Package Servern zu konfigurieren, führen Sie folgende Schritte durch:
   - Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Site Server-Einstellungen".
   - Erweitern Sie im linken Teilfenster "Site-Verwaltung > Einstellungen > Package Service" und klicken Sie dann auf "Package Service-Einstellungen".
   - Klicken Sie auf der Seite "Package Service-Einstellungen" unter "Globale Package Service-Einstellungen" auf "HTTPS-Codebasis veröffentlichen".
   - Klicken Sie auf "Änderungen speichern".
2. Um einen einzelnen Package Server für die Verwendung von HTTPS zu konfigurieren, erstellen Sie den folgenden Registrierungsschlüssel und die Werte auf jedem Package Server-Computer, der sich auf der gleichen Site wie der Notification Server befindet:
   - Registrierungspfad: HKEY_LOCAL_MACHINE \ SOFTWARE \ Altiris \ Altiris Agent \ Package Server
   - Schlüsseltyp: DWORD
   - Name: EnableHTTPSOverride
   - Wert: 1

   Dieser Registrierungsschlüssel übergeht die HTTP-Codebasiskonfiguration auf dem Package Server und veranlasst ihn stattdessen dazu, HTTPS-Codebasen zu veröffentlichen.

Im nächsten Schritt müssen Sie Sites und Site Server zur Verarbeitung von Cloud-fähigen Agents konfigurieren.

Siehe "Konfigurieren von Sites und Site Servern zum Verarbeiten von Cloud-fähigen Agents" auf Seite 317.

Eine detaillierte Beschreibung des Prozesses zum Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung finden Sie unter Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.

Konfigurieren von Sites und Site Servern zum Verarbeiten von Cloud-fähigen Agents

Stellen Sie sicher, dass Sie die Package Server zur Veröffentlichung von HTTPS-Codebasen konfiguriert haben, bevor Sie diesen Schritt ausführen.

Siehe "Konfigurieren eines Package Servers zur Veröffentlichung von HTTPS-Paket-Codebasen" auf Seite 315.

Die Computer, die Sie über das Internet verwalten möchten, sollten in einer oder mehreren Sites organisiert werden. Diese Sites müssen für Cloud-fähige Agents zuständig sein und dürfen keine direkt verwalteten Agents enthalten. Sie sollten anschließend die entsprechenden Site Server jeder Site zuweisen.

Die Cloud-fähige Verwaltung unterstützt Internet-Package Server und Internet-Task Server, auf die der Symantec Management-Agent über ein Internet-Gateway zugreift. Die Cloud-fähige Verwaltung unterstützt auch getrennte Package Server. Dabei handelt es sich um Package Server, die sich in der gleichen Site wie die Cloud-fähigen Agents befinden. Nur die lokalen Agents können auf einen nicht verbundenen Package Server zugreifen, und zwar über eine Direktverbindung. Nicht verbundene Task Server werden jedoch nicht unterstützt.

Cloud-fähige Computer müssen auf Ressourcenzielen basierenden Sites manuell zugewiesen werden. Cloud-fähige Agents erkennen keine Site-Zuweisungen, die auf IP-Adressen und Subnetzen basieren. Durch die manuelle Zuweisung wird sichergestellt, dass jeder Computer Mitglied der entsprechenden Site bleibt, unabhängig davon, wo sich der Computer physisch befindet.

Siehe "Verwalten von Sites" auf Seite 135.

Sie können einen Cloud-fähigen Agent manuell mehreren Sites oder Site Servern zuweisen. Die Site Server, die für den Agent verfügbar sind, bilden die Gesamtheit aller Site Server in den zugewiesenen Sites.

Sie können Ihre Site Server-Einstellungen für Cloud-fähige Agents folgendermaßen konfigurieren:

Erstellen Sie eine Site und konfigurieren Sie sie.	Sie können beliebig viele Sites erstellen und konfigurieren, um der Konfiguration ihrer Umgebung zu entsprechen. Ein Cloud-fähiger Agent oder ein Package Server, der mehreren Sites zugewiesen ist, erhält die Gesamtheit aller Site Server in den zugewiesenen Sites.
Weisen Sie die Cloud-fähigen Agents direkt den Site Servern zu.	Sie weisen ein Ressourcenziel direkt dem Site Server zu, um sicherzustellen, dass die Zielmitglieder nur Zugriff auf diesen bestimmten Site Server erhalten. Durch die Methode der Zuweisung nach Site werden alle Site Server, die Mitglieder der zugewiesenen Site sind, für die als Ziele ausgewählten Cloud-fähigen Agents verfügbar.

Hinweis: Bei Bedarf können Sie diese beiden Zuweisungsmethoden miteinander kombinieren.

Diese Aufgabe ist ein Schritt im Prozess für das Vorbereiten Ihrer Umgebung auf die Cloud-fähige Verwaltung.

Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.

So erstellen Sie eine Internetseite und konfigurieren Sie zur Verarbeitung von Cloud-fähigen Agents

1. Erstellen Sie in der Symantec Management Console eine neue Site.

   Siehe "Verwalten von Sites" auf Seite 135.

2. Weisen Sie das entsprechende Ressourcenziel der Site manuell zu.

   Dieses Ressourcenziel enthält die Cloud-fähigen Agents und die Package Server. Sie können das gleiche Ressourcenziel, das auf die Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" angewendet wurde, wiederverwenden.

3. Weisen Sie die entsprechenden Site Server der Site mithilfe einer der folgenden Methoden zu:

So weisen Sie den Site Server manuell der Site zu	1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Site Server-Einstellungen". 2 Erweitern Sie im linken Teilfenster "Site-Verwaltung > Site Servers > *name_ihres_site_servers* und klicken Sie dann auf "Internetsites". 3 Klicken Sie im rechten Teilfenster unter "Detaillierte Informationen" auf "Neu". 4 Klicken Sie im Dialogfeld "Internetsite auswählen" auf die Internetsite, der Sie den Site Server zuweisen möchten, und klicken Sie dann auf "OK".
So weisen Sie das/die Subnetz(e) der lokalen Site Server der Site zu	1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Site Server-Einstellungen". 2 Klicken Sie im linken Teilfenster auf "Site-Verwaltung > Subnetze". 3 Wählen Sie im rechten Teilfenster das entsprechende Subnetz aus. 4 Klicken Sie in der Symbolleiste auf "Site zuweisen". 5 Wählen Sie im Fenster "Standort auswählen" die Site aus, der Sie das Subnetz zuweisen möchten. **Hinweis:** Ein lokaler Site Server befindet sich in derselben nicht verbundenen Site wie die Cloud-fähigen Agents, die er bearbeitet. Diese Art der Zuweisung macht es erforderlich, dass die nicht verbundene Site ein eindeutiges Subnetz hat, das sich nicht mit Subnetzen von internen Clients überlappt, falls vorhanden. Diese Konfiguration ist nicht üblich, daher wird dieser Ansatz generell nicht empfohlen.

Siehe "Manuelles Zuweisen eines Site Server zu einer Site" auf Seite 140.

So weisen Sie Cloud-fähige Agents direkt einem Site Server zu

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Site Server-Einstellungen".
2. Erweitern Sie im linken Teilfenster den Site Server, den Sie ändern möchten, und klicken Sie anschließend auf "Manuell zugewiesene Agents".
3. Klicken Sie im rechten Teilfenster auf "Neu", geben Sie das Ressourcenziel an, das die entsprechenden Cloud-fähigen Agents enthält, und klicken auf dann "OK".

   Siehe "Auswählen benannter Ressourcenziele" auf Seite 403.

Im nächsten Schritt müssen Sie sicherstellen, dass die Internetsite richtig konfiguriert ist.

Eine detaillierte Beschreibung des Prozesses zum Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung finden Sie unter Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.

Kapitel 20

Einrichten der Cloud-fähigen Verwaltung

In diesem Kapitel werden folgende Themen behandelt:

- Einrichten der Cloud-fähigen Verwaltung

Einrichten der Cloud-fähigen Verwaltung

Bevor Sie diese Funktionen der Cloud-fähigen Verwaltung nutzen können, müssen Sie die Internet-Gateways installieren und konfigurieren. Nachher müssen Sie die Cloud-fähigen Verwaltungsrichtlinien konfigurieren und außerdem die Symantec Management-Agents einrichten, um die Cloud-fähige Verwaltungsumgebung zu unterstützen.

Bevor Sie die Cloud-fähige Verwaltung einrichten können, müssen Sie Ihre Umgebung für den Einsatz von SSL konfigurieren.

Siehe "Vorbereiten Ihrer Umgebung für die Cloud-fähige Verwaltung" auf Seite 300.

Tabelle 20-1 Einrichten der Cloud-fähigen Verwaltung

Schritt	Aktion	Beschreibung
Schritt 1	Vergewissern Sie sich, dass die Einstellungen für den Anwendungspool korrekt sind.	Bei der Cloud-fähigen Verwaltung muss der Anwendungspool "DefaultAppPool" die Einstelllung "Integriert" unter "Verwalteter Pipelinemodus" verwenden. Stellen Sie sicher, dass die Einstellung "Integriert" verwendet wird, bevor Sie mit der Einrichtung der Cloud-fähigen Verwaltung fortfahren. Siehe "Einstellen, dass der Anwendungspool "DefaultAppPool" die Einstellung "Integriert" unter "Verwalteter Pipelinemodus" verwendet" auf Seite 324.

Schritt	Aktion	Beschreibung
Schritt 2	Einstellungen für die Cloud-fähige Management-Agent-IIS-Website konfigurieren	Eine separate Agent-Site auf dem Notification Server ist für Cloud-fähige Agents erforderlich. Diese Site enthält nur Agent-Schnittstellen und bietet keinen Zugriff auf die Seiten der Symantec Management Console. Sie führt auch zusätzliche Zertifikat- und Ressourcenzugriffsprüfungen durch, um Sicherheitsmaßnahmen für die Agents durchzusetzen, die über das Internet eine Verbindung herstellen. Sie müssen das Internet-Gateway konfigurieren, um nur den Zugriff auf die Agent-Site auf dem Notification Server zu ermöglichen. Siehe "Konfigurieren der Einstellungen für die Cloud-fähige Management-Agent IIS-Website" auf Seite 324.
Schritt 3	Internet-Gateway-Computer vorbereiten	Der Internet-Gateway-Computer sollte sich in der DMZ Ihres Unternehmens befinden, um sicherzustellen, dass er vor externen und internen Netzwerken geschützt ist. Sie müssen die Firewall auf dem Gateway-Computer so konfigurieren, dass eingehende Verbindungen aus dem Internet nur am entsprechenden Gateway-Port zugelassen werden. Außerdem müssen Sie die Firewall so konfigurieren, dass ausgehende Verbindungen nur zu bestimmten Servern in Ihrem internen Netzwerk zugelassen werden. Wird das Gateway auf einem virtuellen VMware-Computer ausgeführt, sollten Sie den Netzwerkadapter VMXNET 3 verwenden. Beachten Sie, dass VMXNET 3 nur verfügbar ist, wenn Sie VMware-Tools haben, die auf Ihrem virtuellen Computer installiert werden. Weitere Informationen zum VMXNET 3-Netzwerkadapter finden Sie im folgenden VMware-Dokument der Supportdatenbank: KB1001805. Auf dem Computer muss das Betriebssystem Windows Server 2008 R2 SP1 mit der Funktion .NET Framework 3.5.1 aktiv sein. Die Symantec Management-Plattform muss den Gateway-Computer nicht verwalten. Das Internet-Gateway ist normalerweise nicht verwaltet. Bevor Sie die Installation starten, sollten Sie überprüfen, ob der Gateway-Computer auf den Notification Server-Computer und auf alle erforderlichen Site Server-Computer zugreifen kann. Verwenden Sie beim Überprüfen der Verbindung die Hostnamen, den FQDN oder die IP-Adressen, mit denen die Cloud-fähigen Agents eine Verbindung herzustellen versuchen. Siehe "Info zum Vorbereiten des Internet-Gateway-Computers" auf Seite 327.

Schritt	Aktion	Beschreibung
Schritt 4	Laden Sie das Internet-Gateway-Installationspaket herunter und führen Sie es aus.	Um das Internet-Gateway zu installieren, müssen Sie das Internet-Gateway-Installationspaket von der Symantec Management Console herunterladen und ausführen. Siehe "Herunterladen und Ausführen das Internet-Gateway-Installationspakets" auf Seite 329.
Schritt 5	Konfigurieren Sie das Internet-Gateway mithilfe des Assistenten zum Konfigurieren des Internet-Gateway der Symantec Management-Plattform und des Internet-Gateway-Managers der Symantec Management-Plattform.	Geben Sie im Assistenten zum Konfigurieren des Internet-Gateway der Symantec Management-Plattform den Port für eingehende Verbindungen, die Informationen zum SSL-Zertifikat und das Benutzerkonto an. Fügen Sie im Internet-Gateway-Manager der Symantec Management-Plattform Ihren Notification Server und Ihre Site Server der Liste der Server hinzu, die mit dem Internet-Gateway kommunizieren können. Sie müssen auch den Gateway-Zertifikatsfingerabdruck kopieren, den Sie für das Konfigurieren der Richtlinie "Cloud-fähige Verwaltungseinstellungen" benötigen. Siehe "Konfigurieren des Internet-Gateway" auf Seite 331.
Schritt 6	Konfigurieren Sie die Richtlinie "Cloud-fähige Verwaltungseinstellungen".	Mithilfe der Richtlinie "Cloud-fähige Verwaltungseinstellungen" können Sie die Computer ansteuern, die über das Internet verwaltet werden sollen. Außerdem enthält die Richtlinie die Liste der Internet-Gateways, die für die angesteuerten Clientcomputer verfügbar sind. Siehe "Konfigurieren der Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" Richtlinie konfigurieren" auf Seite 334. Um die vorhandenen Symantec Management-Agents in die Cloud-fähige Verwaltung aufzunehmen, müssen Sie die entsprechenden Computer der Richtlinie "Cloud-fähige Verwaltungseinstellungen" hinzufügen.
Schritt 7	Installieren Sie den Symantec Management-Agent auf getrennten Computern.	In einigen Fällen hat ein Computer, den Sie verwalten möchten, möglicherweise keinen Zugriff auf das Netzwerk, das die Symantec Management-Plattform hostet. Um den Symantec Management-Agent auf einem getrennten Computer zu installieren, müssen Sie das Agent-Installationspaket von Ihrer Symantec Management Console herunterladen, auf geeigneten Medien speichern und es anschließend auf den entsprechenden Computern installieren. Siehe "Installieren des Symantec Management-Agent auf einem nicht verbundenen Computer" auf Seite 338.

Einstellen, dass der Anwendungspool "DefaultAppPool" die Einstellung "Integriert" unter "Verwalteter Pipelinemodus" verwendet

Bei der Cloud-fähigen Verwaltung muss der Anwendungspool "DefaultAppPool" die Einstelllung "Integriert" unter "Verwalteter Pipelinemodus" verwenden.

Diese Aufgabe ist ein Schritt im Prozess für das Einrichten der Cloud-fähigen Verwaltung.

Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

So legen Sie fest, dass der Anwendungspool "DefaultAppPool" die Einstellung "Integriert" unter "Verwalteter Pipelinemodus" verwendet.

1. Öffnen Sie auf dem Notification Server-Computer den "Internet Information Services (ISS) Manager".
2. Klicken Sie im "Internet Information Services (ISS) Manager" im Bereich "Verbindungen" auf "(Name des Notification Server-Computers) > Anwendungspools".
3. Klicken Sie im Bereich "Anwendungspools" auf "DefaultAppPool" und anschließend im Bereich "Aktionen" auf "Grundeinstellungen".
4. Wählen Sie im Fenster "Anwendungspool bearbeiten" unter "Verwalteter Pipelinemodus" "Integriert". Klicken Sie dann auf "OK".

Im nächsten Schritt müssen Sie die Richtlinie "Einstellungen für die Cloud-fähige Management-Agent-Website" konfigurieren.

Siehe "Konfigurieren der Einstellungen für die Cloud-fähige Management-Agent IIS-Website" auf Seite 324.

Eine detaillierte Beschreibung des Prozesses zum Einrichten der Cloud-fähigen Verwaltung finden Sie unter Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

Konfigurieren der Einstellungen für die Cloud-fähige Management-Agent IIS-Website

Stellen Sie sicher, dass der Anwendungspool "DefaultAppPool" die Einstellung "Integriert" unter "Verwalteter Pipelinemodus" verwendet, bevor Sie diesen Schritt ausführen.

Siehe "Einstellen, dass der Anwendungspool "DefaultAppPool" die Einstellung "Integriert" unter "Verwalteter Pipelinemodus" verwendet" auf Seite 324.

Eine separate Agent-Site auf dem Notification Server ist für Cloud-fähige Agents erforderlich. Diese Site enthält nur Agent-Schnittstellen und bietet keinen Zugriff auf die Seiten der Symantec Management Console. Sie führt auch zusätzliche

Zertifikat- und Ressourcenzugriffsprüfungen durch, um Sicherheitsmaßnahmen für die Agents durchzusetzen, die über das Internet eine Verbindung herstellen.

Diese Aufgabe ist ein Schritt beim Einrichten der Cloud-fähigen Verwaltung.

Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

So konfigurieren Sie die Einstellungen für die Cloud-fähige Management-Agent IIS-Website

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Notification Server > Cloud-fähige Verwaltung".
2. Erweitern Sie im linken Teilfenster den Ordner "Einrichten" und klicken Sie anschließend auf "Einstellungen für die Cloud-fähige Management-Agent-IIS-Website".

3 Aktivieren Sie auf der Seite "Einstellungen für die Cloud-fähige Management-Agent-Website" die Option "IIS-Website für Cloud-fähige Management-Agent-Verbindungen hinzufügen" und nehmen Sie folgende Einstellungen vor:

Name	Hier können Sie den Namen angeben, unter dem die Website im "Internet Information Services (IIS) Manager" angezeigt wird.
Port	Hier geben Sie den Port an, auf dem die Website verfügbar sein wird. Für die Einrichtung der Cloud-fähigen Verwaltung muss der Internet-Gateway-Computer auf den ausgewählten Port zugreifen können.
FQDN	Zeigt den derzeitigen FQDN des Notification Server-Computers an.
Zertifikat	Damit können Sie ein kommerzielles SSL-Zertifikat importieren oder ein selbstsigniertes SSL-Zertifikat erstellen.

4 Klicken Sie auf "Änderungen speichern".

Hinweis: Eine Paketaktualisierungsaufgabe ist Teil des Erstellungsprozesses der Website. In Umgebungen mit zahlreichen solcher Aufgaben kann deren Ausführung viel Zeit in Anspruch nehmen. Nach der Protokollierung der folgenden Meldungen können Sie die Symantec Management Console sicher schließen:

```
Aufgabe zur Erstellung eine Agent-Site {Task_Guid} wurde begonnen.

Paketaktualisierung für alle Pakete begonnen.
```

Die Cloud-fähige Management-Agent-IIS-Site erfordert eine Verbindung, die mit einem SSL-Zertifikat gesichert ist. Sie können entweder ein kommerzielles Zertifikat importieren oder ein selbstsigniertes Zertifikat erstellen. Ein kommerzielles Zertifikat muss die folgenden Anforderungen erfüllen:

Tabelle 20-2 Symantec Management-Plattform-Anforderungen für SSL-Zertifikate

Digitale Signatur	Das Zertifikat hat eine gültige digitale Signatur.

Vertrauen	Das Zertifikat wird von der Zertifizierungsstelle ausgestellt, die vom Notification Server-Computer als vertrauenswürdig eingestuft wird.
Gültigkeit	Das Zertifikat ist mindestens 30 Tage ab dem Importdatum gültig.
Erweiterte Schlüsselverwendung	Der Wert "Erweiterte Schlüsselverwendung" des Zertifikats ist Serverauthentifizierung-OID (1.3.6.1.5.5.7.3.1).
Antragstellername oder alternativer Antragstellername	Der Antragstellername oder der alternative Antragstellername stimmt mit dem vollqualifizierten Domänennamen (FQDN) des Notification Server-Computers überein.
Hash-Algorithmus	Das Zertifikat verwendet einen der folgenden Hash-Algorithmen: ■ SHA1 ■ SHA256 ■ SHA384 ■ SHA512
Asymmetrischer Algorithmus	Das Zertifikat verwendet den asymmetrischen RSA-Algorithmus.
Dateiformat	.pfx

Im nächsten Schritt müssen Sie den Computer vorbereiten.

Siehe "Info zum Vorbereiten des Internet-Gateway-Computers" auf Seite 327.

Eine detaillierte Beschreibung des Prozesses zum Einrichten der Cloud-fähigen Verwaltung finden Sie unter Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

Info zum Vorbereiten des Internet-Gateway-Computers

Stellen Sie sicher, dass Sie die IIS-Website-Einstellungen des Agents der Cloud-fähigen Verwaltung konfiguriert haben, bevor Sie diesen Schritt ausführen.

Siehe "Konfigurieren der Einstellungen für die Cloud-fähige Management-Agent IIS-Website" auf Seite 324.

Über das Internet-Gateway können Symantec Management-Agents im Internet mit der Symantec Management-Plattform kommunizieren. Das Internet-Gateway leitet Anforderung von authentifizierten Symantec Management-Agents an bestimmte Port-Nummern auf Notification Server-Instanzen oder an Site Server hinter dem

Gateway weiter. Standardmäßig werden alle Anforderungen vom Standard-HTTPS-Port 443 auf dem Gateway an Port 4726 auf dem Notification Server-Computer weitergeleitet.

Das Internet-Gateway erstellt durch die interne Firewall einen virtuellen Tunnel. Es ermöglicht autorisierten Clients im Internet den Zugriff auf die entsprechenden internen Server, aber es blockiert alle nicht autorisierten Clients. Der Cloud-fähige Symantec Management-Agent kommuniziert über das Internet direkt mit dem Gateway. Es ist kein VPN erforderlich. Wenn ein Cloud-fähiger Agent eine Verbindung herstellt, tauschen das Gateway und der Agent ihre Zertifikate aus und überprüfen sich gegenseitig. Das Gateway prüft, ob ein bekannter Notification Server das Agentzertifikat ausgestellt hat. Das Gateway erstellt dann einen Tunnel, über den der Agent direkt mit dem entsprechenden Notification Server bzw. den entsprechenden Site Servern unter Verwendung von HTTPS kommunizieren kann. Wenn der Agent die Kommunikation mit dem Zielserver beendet hat, schließt er seine Verbindung zum Gateway und anschließend löscht das Gateway den Tunnel.

Die Cloud-fähige Verwaltung unterstützt keine Verwendung von Proxy-Servern. Sie können zwischen Cloud-aktivierten Symantec Management-Agent und Internet-Gateway kein Proxy einrichten.

Symantec empfiehlt, dass Sie mindestens zwei Internet-Gateways konfigurieren, um Failoveroptionen und Lastverteilung bereitzustellen und eine Aufrechterhaltung der Verbindung zu gewährleisten. Jedes Internet-Gateway kann mehrere Notification Server verarbeiten. Diese Konfiguration wird unterstützt, selbst wenn Notification Server in einer Hierarchiestruktur organisiert werden. Jedes Internet-Gateway unterstützt bis zu 60.000 Endgeräte und 3.000 gleichzeitige Verbindungen.

Die folgenden Beispiele helfen Ihnen bei der Entscheidung, wie viele Internet-Gateways Sie in Ihrer Umgebung benötigen:

- Wenn Sie 20.000 Clients auf einem Notification Server haben und 30% von ihnen Cloud-fähig sind, ist es am besten, über zwei Internet-Gateways zu verfügen, um eine hohe Verfügbarkeit zu gewährleisten. Ein Internet-Gateway ist jedoch auch in der Lage, diese Konfiguration leicht zu bearbeiten.
- Wenn Sie über 180.000 Clients aufgeteilt auf zwei Hierarchien verfügen und 70 % davon Cloud-fähig sind, benötigen Sie mindestens vier Internet-Gateways: drei, um die Knotenlast zu bearbeiten und eins für die Fehlertoleranz.

Bevor Sie das Internet-Gateway installieren, müssen Sie den Hostcomputer konfigurieren. Der Gateway-Computer sollte sich in der DMZ Ihrer Organisation befinden, um sicherzustellen, dass er vor externen und internen Netzwerken geschützt ist. Sie müssen die Firewall auf dem Gateway-Computer so konfigurieren, dass eingehende Verbindungen aus dem Internet nur an den entsprechenden Gateway-Ports zugelassen werden. Außerdem müssen Sie die Firewall so

konfigurieren, dass ausgehende Verbindungen nur zu bestimmten Servern in Ihrem internen Netzwerk zugelassen werden.

Wird das Gateway auf einem virtuellen VMware-Computer ausgeführt, sollten Sie den Netzwerkadapter VMXNET 3 verwenden. Beachten Sie, dass VMXNET 3 nur verfügbar ist, wenn Sie VMware-Tools haben, die auf Ihrem virtuellen Computer installiert werden. Weitere Informationen zum VMXNET 3-Netzwerkadapter finden Sie im folgenden VMware-Dokument der Supportdatenbank: KB1001805.

Hinweis: Der Internet-Gateway-Computer muss das Betriebssystem "Windows Server 2008s R2 SP1" haben und die Funktion ".NET-Frameworks 3.5.1" muss aktiviert sein.

Die Symantec Management-Plattform muss nicht den Gateway-Computer verwalten. Das Internet-Gateway ist gewöhnlich nicht verwaltet.

Bevor Sie die Installation beginnen, prüfen Sie, dass der Internet-Gateway-Computer auf den Notification Server-Computer sowie alle erforderlichen Site Server-Computer zugreifen kann. Verwenden Sie beim Überprüfen der Verbindung die Hostnamen oder die IP-Adressen, mit denen die Cloud-fähigen Agents versuchen, Verbindungen herzustellen.

Diese Aufgabe ist ein Schritt im Prozess für das Einrichten der Cloud-fähigen Verwaltung.

Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

Siehe "Info zur Internet-Gateway-Lastverteilung" auf Seite 543.

Im nächsten Schritt müssen Sie das Installationspaket für das Internet-Gateway herunterladen.

Siehe "Herunterladen und Ausführen das Internet-Gateway-Installationspakets" auf Seite 329.

Eine detaillierte Beschreibung des Prozesses zum Einrichten der Cloud-fähigen Verwaltung finden Sie unter Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

Herunterladen und Ausführen das Internet-Gateway-Installationspakets

Stellen Sie sicher, dass Sie den Internet-Gateway-Computer vorbereitet haben, bevor Sie diesen Schritt ausführen.

Siehe "Info zum Vorbereiten des Internet-Gateway-Computers" auf Seite 327.

Wenn Sie ein neues Internet-Gateway installieren möchten, müssen Sie zuerst das entsprechende Internet-Gateway-Installationspaket beziehen. Das Installationspaket ist eine ausführbare Datei, die Sie über die Symantec Management Console herunterladen können. Das Paket enthält ein Installationsprogramm, das Sie durch den Installationsprozess führt.

Wenn Sie vom Gateway-Computer aus per Fernzugriff auf die Symantec Management Console zugreifen können, haben Sie die Möglichkeit, das Internet-Gateway-Installationspaket direkt auszuführen. Alternativ können Sie die Datei auf einem beliebigen anderen Medium speichern, sie auf den entsprechenden Internet-Gateway-Computer kopieren und dann ausführen.

Warnung: Schließen Sie alle Windows-Programme, bevor Sie das Internet-Gateway-Installationspaket ausführen.

Diese Aufgabe ist ein Schritt im Prozess für das Einrichten der Cloud-fähigen Verwaltung.

Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

So laden Sie das Internet-Gateway-Installationspaket herunterladen und führen es aus

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Cloud-fähige Verwaltung".
2. Erweitern Sie im linken Teilfenster "Setup" und klicken Sie dann auf "Cloud-fähige Verwaltung einrichten".
3. Klicken Sie auf der Seite "Cloud-fähige Verwaltung einrichten" auf der Registerkarte "Internet-Gateway einrichten" auf "Installationspaket für Internet-Gateway herunterladen"
4. Wenn Sie auf dem Gateway-Computer sind, können Sie auf "Ausführung" klicken, um das Installationsprogramm sofort auszuführen.

   Wenn Sie das Paket als Datei speichern möchten, um es später oder auf einen anderen Computer auszuführen, klicken Sie auf "Speichern", geben Sie den entsprechenden Ordner an und klicken Sie dann auf "OK".
5. Navigieren Sie zum Installationspaket für das SMP-Internet-Gateway, das Sie heruntergeladen haben, und doppelklicken Sie auf `SMP_Internet_Gateway`.
6. Klicken Sie im Dialogfeld "Datei öffnen – Sicherheitswarnung" auf "Ausführung".
7. Klicken Sie im Dialogfeld "Internet Gateway für Symantec Management-Plattform einrichten" auf "Weiter".
8. Klicken Sie auf "Ich akzeptiere die Lizenzvereinbarung" und dann auf "Weiter".

9 Geben Sie den Pfad zum Zielordner an, in dem Sie die Internet-Gateway-Dateien installieren möchten, klicken Sie auf "Weiter" und dann auf "Weiter".

10 Stellen Sie sicher, dass "Konfigurationsassistent starten" aktiviert ist und klicken Sie dann auf "Fertig stellen".

Im nächsten Schritt müssen Sie das Internet-Gateway konfigurieren.

Siehe "Konfigurieren des Internet-Gateway" auf Seite 331.

Eine detaillierte Beschreibung des Prozesses zum Einrichten der Cloud-fähigen Verwaltung finden Sie unter Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

Konfigurieren des Internet-Gateway

Stellen Sie sicher, dass Sie das Installationspaket für das Internet-Gateway heruntergeladen haben, bevor Sie diesen Schritt ausführen.

Siehe "Herunterladen und Ausführen das Internet-Gateway-Installationspakets" auf Seite 329.

Nachdem das Internet-Gateway installiert ist, müssen Sie es konfigurieren, damit es mit der Symantec Management-Plattform zusammenarbeitet. Sie konfigurieren das Internet-Gateway unter Verwendung des "Assistenten zum Konfigurieren des Internet-Gateway der Symantec Management-Plattform" und des "Internet-Gateway-Managers der Symantec Management-Plattform".

Im "Assistenten zum Konfigurieren des Internet-Gateway der Symantec Management-Plattform" geben Sie den Port für eingehende Verbindungen, die SSL-Zertifikatinformationen und das Benutzerkonto ein.

Im "Internet-Gateway-Manager der Symantec Management-Plattform" fügen Sie Ihren Notification Server und Ihre Site Server der Liste der Server hinzu, die mit dem Internet-Gateway kommunizieren können. Sie rufen außerdem den Gateway-Zertifikatsfingerabdruck ab, den Sie für das Konfigurieren der Richtlinie "Cloud-fähige Verwaltungseinstellungen" benötigen.

Diese Aufgabe ist ein Schritt beim Einrichten der Cloud-fähigen Verwaltung.

Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

So konfigurieren Sie das Internet-Gateway unter Verwendung des Assistenten zum Konfigurieren des Internet-Gateway der Symantec Management-Plattform

1. Geben Sie auf dem Internet-Gateway-Computer im Assistenten zum Konfigurieren des Internet-Gateway der Symantec Management-Plattform auf der Seite "IP-Adressen und Ports" die entsprechenden Werte an und klicken Sie dann auf "Weiter".

   Standardmäßig ist der Port für eingehende Verbindungen 443. Sie können jedoch bei Bedarf eine andere Port-Nummer angeben. Alle angegebenen Port-Nummern müssen TCP-Ports sein (nummeriert von 1 bis 65535).

   Sie sollten die IP-Adresse des Internet-Gateway-Computers verwenden. Sie können nur eine Port-Nummer und nur eine IP-Adresse angeben. Wenn Sie beschließen, alle verfügbaren IP-Adressen zu verwenden, wird dieselbe Port-Nummer für alle IP-Adressen verwendet. Wenn Sie eine granularere Steuerung von IP-Adressen und Port-Nummern benötigen, müssen Sie die Apache-Konfigurationsdatei direkt bearbeiten.

2. Auf der Seite "SSL-Zertifikatinformationen" geben Sie die entsprechenden Zertifikatsinformationen an und klicken Sie dann auf "Weiter".

   Das Internet-Gateway muss ein verfügbares SSL-Zertifikat haben, damit Symantec Management-Agents mit ihm kommunizieren können. Der Konfigurationsassistent generiert ein selbstsigniertes SSL-Zertifikat, das auf den angegebenen Informationen basiert.

   Bei Bedarf können Sie Ihr eigenes Zertifikat anstelle des generierten selbstsignierten Zertifikats verwenden. Sie müssen das Zertifikat und die Schlüsseldateien nach der Installation manuell ersetzen.

   Erstellen Sie ein Zertifikat und einen privaten Schlüssel oder rufen Sie diese von einer Zertifizierungsstelle ab. Speichern Sie Zertifikat und Schlüssel in `%installdir%\Apache\certs\server.crt` bzw. `%installdir%\Apache\certs\server.key`. Zertifikat und Schlüssel sollten im Format "pem -nodes" gespeichert werden und eine vollständige Zertifizierungsfolge enthalten. Starten Sie dann entweder Apache (`httpd.exe`) neu oder die Software, um den Dienst neu zu starten.

3. Auf der Site "Benutzerkonto" geben Sie die entsprechenden Benutzerkontoinformationen ein und klicken Sie dann auf "Weiter".

   Aus Sicherheitsgründen sollten Sie den Internet-Gateway-Dienst als zugeordnetes Benutzerkonto ausführen. Symantec empfiehlt die Verwendung des Kontos "LocalService".

4. Auf der Seite "Übersicht" überprüfen Sie die Einstellungen und klicken Sie dann auf "Fertig stellen".

So konfigurieren Sie das Internet-Gateway im "Internet-Gateway-Manager der Symantec Management-Plattform"

1. Klicken Sie zum Öffnen des "Internet-Gateway-Manager der Symantec Management-Plattform" auf "Start > Programme > Symantec > Internet-Gateway-Manager".

   Beachten Sie, dass nach Abschluss des Assistenten zum Konfigurieren des Internet-Gateway der "Internet-Gateway-Manager der Symantec Management-Plattform" automatisch geöffnet.

2. So fügen Sie Ihre Site Server und Notification Server der Liste von Servern hinzu, die mit dem Internet-Gateway kommunizieren können:

   - Klicken Sie im Internet-Gateway-Manager der Symantec-Management-Platform auf der Registerkarte "Server" auf "Server hinzufügen".
   - Fügen Sie im Dialogfeld "Server hinzufügen" einen Hostnamen hinzu und bearbeiten Sie bei Bedarf die Nummer des "SSL-Port". Wenn Sie einen Notification Server hinzufügen, stellen Sie sicher, dass die Option "Dies ist ein SMP-Server" aktiviert ist. Klicken Sie auf "OK".
     Beachten Sie, dass der SSL-Port des Notification Server-Computers mit dem in der Symantec Management Console auf der Seite "CEM-Agent-Site-Einstellungen" übereinstimmen muss.
   - Wenn das Dialogfeld "Zertifikatswarnung" angezeigt wird, klicken Sie auf "Ignorieren".
   - Klicken Sie im Dialogfeld "Dienst neu starten?" auf "Ja".

3. Klicken Sie zum Kopieren des Gateway-Zertifikatsfingerabdrucks, den Sie zum Konfigurieren der Richtlinie "Cloud-fähige Verwaltungseinstellungen" in der Symantec Management Console benötigen, im Internet-Gateway-Manager der Symantec Management-Plattform auf der Registerkarte "Allgemein" auf "In Zwischenablage kopieren".

   Siehe "Konfigurieren der Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" Richtlinie konfigurieren" auf Seite 334.

Siehe "Internet-Gateway-Verwaltungsskripts" auf Seite 542.

Im nächsten Schritt müssen Sie die Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" konfigurieren.

Siehe "Konfigurieren der Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" Richtlinie konfigurieren" auf Seite 334.

Eine detaillierte Beschreibung des Prozesses zum Einrichten der Cloud-fähigen Verwaltung finden Sie unter Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

Konfigurieren der Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" Richtlinie konfigurieren

Stellen Sie sicher, dass Sie das Internet-Gateway konfiguriert haben, bevor Sie diesen Schritt ausführen.

Siehe "Konfigurieren des Internet-Gateway" auf Seite 331.

Mithilfe der Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" können Sie die spezifischen Computer auswählen, die Sie über das Internet verwalten möchten. Die Richtlinie enthält die Liste mit Internet-Gateways, die den Ziel-Clientcomputern zur Verfügung stehen. Sie können die verfügbaren Internet-Gateways festlegen, indem Sie die entsprechenden Details zu jedem Gateway angeben.

Sie würden normalerweise nur eine Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" konfigurieren. Sie benötigen nur dann mehrere Richtlinien, wenn Sie genauer steuern möchten, welche Internet-Gateways welche Cloud-fähigen Computer verarbeiten oder wenn Sie einen manuellen Lastenausgleich durchführen möchten.

Um ein Agent-Installationspaket zu generieren, müssen Sie eine Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" erstellen oder auswählen und sie auf die entsprechenden Zielcomputer anwenden. Die Liste der für die ausgewählte Richtlinie verfügbaren Internet-Gateways ist im Agent-Installationspaket enthalten. Diese Liste ermöglicht es dem neu installierten Agent, die Kommunikation mit dem Notification Server sofort zu beginnen. Der neue Cloud-fähige Computer wird automatisch zum Ressourcenziel der ausgewählten Richtlinie hinzugefügt.

Wenn Symantec Management Agent die Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" erhält und er keine direkte Verbindung zum Notification Server hergestellt hat, versucht er, eine Verbindung über das Internet-Gateway herzustellen. Wenn der Agent erfolgreich eine Verbindung hergestellt hat, wird er zu einem Cloud-fähigen Agent. Der Symantec Management-Agent wechselt nur dann in den Cloud-fähigen Modus, wenn er über das Gateway erfolgreich eine Verbindung hergestellt hat.

Beachten Sie, dass ein Cloud-fähiger Computer automatisch zur direkten Kommunikation mit dem lokalen Notification Server zurückkehrt, wenn direkter Netzwerkzugriff verfügbar ist. Er wechselt auch automatisch zurück in den Cloud-fähigen Modus, wenn die Direkte Verbindung nicht mehr verfügbar ist. Beispiel: Ein Laptop, der normalerweise an Remote-Standorten eingesetzt wird,

wird unter Umständen gelegentlich im Büro verwendet und mit dem internen Netzwerk verbunden.

Während die Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" auf einen spezifischen Computer abzielt, setzt der Computer die Kommunikation über entsprechende Internet-Gateways fort. Wenn das interne Netzwerk korrekt konfiguriert ist, bleibt der gesamte Datenverkehr zwischen Agent, Internet-Gateway und Notification Server innerhalb des internen Netzwerks. Wenn jedoch die Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" deaktiviert wird oder nicht mehr auf den spezifischen Computer abzielt, verwendet der Computer nicht mehr das Internet-Gateway. Der Computer kehrt zur direkten Kommunikation mit dem lokalen Notification Server zurück.

Ein Cloud-fähiger Agent führt eine Liste mit Internet-Gateways, die zur Verwendung verfügbar sind. Er verwaltet auch eine Liste lokaler und Remote-Site Server, die er verwenden kann. Diese Listen werden auf dem Agent aktualisiert, jedes Mal wenn die Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" aktualisiert wird.

Diese Aufgabe ist ein Schritt im Prozess für das Einrichten der Cloud-fähigen Verwaltung.

Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

So konfigurieren Sie die Richtlinie "Einstellungen für die Cloud-fähige Verwaltung"

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Cloud-fähige Verwaltung".
2. Erweitern Sie im linken Teilfenster "Richtlinie" und klicken Sie dann auf "Einstellungen für die Cloud-fähige Verwaltung".
3. Auf der Seite "Einstellungen für die Cloud-fähige Verwaltung" konfigurieren Sie die Richtlinie wie folgt:

Richten Sie die Liste der Internet-Gateways ein, die externen Agent-Datenverkehr akzeptieren.	Um ein Internet-Gateway hinzuzufügen, geben Sie im Dialogfeld "Gateway-Server bearbeiten" seine Parameter wie folgt an: ■ Server Der vollständig qualifizierter Domänenname (FQDN) des Internet-Gateway-Computers. ■ Port Die Portnummer, die der Symantec Management-Agent verwenden muss, um eine Verbindung mit dem Internet-Gateway herstellen zu können. Der Standardport ist 443. ■ Fingerabdruck Fügen Sie den Wert des Gateway-Zertifikatsfingerabdruck ein, den Sie vom Internet-Gateway-Computer, im "Internet-Gateway-Manager der Symantec Management-Plattform ", auf der Registerkarte "Allgemein" kopiert haben. Siehe "Konfigurieren des Internet-Gateway" auf Seite 331.

Geben Sie die Computer an, für die die Richtlinie gilt.	Wenn Sie die vorhandenen Symantec Management-Agents unter Cloud-fähige Verwaltung bringen möchten, müssen Sie diese Computer der Richtlinie hinzufügen. Nachdem der Agent auf einem Clientcomputer die Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" erhält, stellt er zum Notification Server eine Verbindung her und fordert sein eindeutiges Clientzertifikat an. Wenn der Agent sein Zertifikat erhalten und über keine direkte Verbindung zum Notification Server verfügt, versucht er, über die verfügbaren in der Richtlinie angegebenen Internet-Gateways eine Verbindung herzustellen. Nachdem der Agent erfolgreich eine Verbindung hergestellt hat, wechselt er vom direkt verwalteten Modus und wird ein Cloud-fähiger Agent. **Warnung:** Wenn Sie planen, das Installationspaket zu verwenden, um Agents auf getrennten Computern zu installieren, müssen Sie jene Clients in die Richtlinie mit einbeziehen. Wenn Sie das nicht tun, werden die Gateway-Einstellungen für diese Clients gelöscht, wenn sie eine direkte Verbindung zum lokalen Netzwerk herstellen. Die Gateway-Einstellungen für die Clients werden gelöscht, weil sie nicht automatisch Mitglieder der Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" sind. Sie sollten deshalb den Bereich von Clients definieren, bevor Sie ein Rollout für das Installationspaket ausführen. Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

4 Aktivieren Sie die Richtlinie.

   Klicken Sie oben rechts auf der Seite auf den farbigen Kreis und dann auf "Ein".

5 Klicken Sie auf "Änderungen speichern".

   Nachdem Symantec Management-Agent die Richtlinie erhält, kann er die Cloud-fähige Verwaltung verwenden. Bis der Clientcomputer zum internen Netzwerk eine Verbindung hergestellt hat, bleibt die Cloud-fähige Verwaltung deaktiviert. Wenn Sie den Clientcomputer vom internen Netzwerk trennen und der Symantec Management-Agent in der Lage ist, über ein Internet-Gateway eine Verbindung zum Notification Server herzustellen, wird die Cloud-fähige Verwaltung automatisch aktiv.

   Sie können den Status des Modus "Cloud-fähige Verwaltung" im Symantec Management-Agent des Clientcomputers auf der Registerkarte "Symantec Management-Agent-Einstellungen" unter "Netzwerkstatus" prüfen.

Im nächsten Schritt installieren Sie den Symantec Management-Agent auf einem nicht verbundenen Computer.

Siehe "Installieren des Symantec Management-Agent auf einem nicht verbundenen Computer" auf Seite 338.

Eine detaillierte Beschreibung des Prozesses zum Einrichten der Cloud-fähigen Verwaltung finden Sie unter Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

Installieren des Symantec Management-Agent auf einem nicht verbundenen Computer

Stellen Sie sicher, dass Sie die Einstellungsrichtlinie für die Cloud-fähige Verwaltung konfiguriert haben, bevor Sie diesen Schritt ausführen.

Siehe "Konfigurieren der Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" Richtlinie konfigurieren" auf Seite 334.

In einigen Fällen hat ein Computer, den Sie verwalten möchten, möglicherweise keinen Zugriff auf das Netzwerk, das die Symantec Management-Plattform hostet. Um den Symantec Management-Agent auf einem nicht verbundenen Computer installieren zu können, müssen Sie zuerst das Agent-Installationspaket von Ihrer Symantec Management Console herunterladen.

Siehe "Parameter für Installationspakete Cloud-fähiger Agents" auf Seite 544.

Nachdem Sie das Installationspaket des Agent von der entsprechenden Instanz der Symantec Management-Plattform generiert haben, müssen Sie es an die nicht verbundene Remote-Site senden. Sie können das Paket per E-Mail oder mit einem

physischen Medium wie einer CD oder einem Flash-Laufwerk senden. Der Benutzer an der Remote-Site führt dann das Agent-Installationspaket aus, um den Symantec Management-Agent auf seinem Computer zu installieren. Der neu installierte Symantec Management-Agent stellt sofort über das entsprechende Internet-Gateway eine Verbindung zum Notification Server her. Sie können das gleiche Installationspaket verwenden, um den Symantec Management-Agent auf allen Computern an einem bestimmten Remote-Standort zu installieren. Jedoch nutzen alle neu installierten Agents dieselben Einstellungen gemeinsam. Verwenden Sie also dieselben Internet-Gateways, um eine Verbindung zum gleichen Notification Server herzustellen.

Hinweis: Wenn Sie Agents auf nicht verbundenen Computern mithilfe des Installationspakets installieren möchten, müssen Sie eine Richtlinie erstellen, die diese Clients mit einschließt. Wenn Sie nicht das tun, werden die Gateway-Einstellungen für diese Clients gelöscht, wenn sie zum lokalen Netzwerk eine direkte Verbindung herstellen. Die Gateway-Einstellungen für die Clients werden gelöscht, weil sie keine Mitglieder der Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" sind. Deshalb sollten Sie den Bereich von Clients vor dem Rollout des Installationspakets definieren.

Diese Aufgabe ist ein Schritt im Prozess für das Einrichten der Cloud-fähigen Verwaltung.

Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

So installieren Sie den Symantec Management-Agent auf einem nicht verbundenen Computer

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Cloud-fähige Verwaltung".
2. Erweitern Sie im linken Teilfenster "Setup" und klicken Sie dann auf "Cloud-fähige Verwaltung einrichten".
3. Klicken Sie auf der Seite "Cloud-fähige Verwaltung einrichten" auf der Registerkarte "Konfiguration von Symantec Management-Agent" auf "Installationspaket für Symantec Management-Agent erzeugen und herunterladen".
4. Geben Sie im Dialogfeld "Installationspaket für den Cloud-fähigen Agent" die entsprechenden Paketparameter an.

   Für weitere Informationen klicken Sie auf die Seite und drücken Sie dann "F1".

   Siehe Tabelle C-5 auf Seite 544.
5. Klicken Sie auf "Agent-Installationspaket generieren".

Die Paketgeneration dauert möglicherweise einige Minuten. Wenn das Paket bereit ist, werden Sie aufgefordert, die Datei auszuführen oder zu speichern.

Das generierte Installationspaket ist ein selbstentpackendes Agent-Installationspaket, das die folgenden Komponenten und Einstellungen umfasst:

- Das Symantec Management-Agent-Installationsprogramm für die entsprechende Plattform.
- Notification Server-Adresse (einschließlich Protokoll und Portnummer, das/die verwendet werden soll).
- Notification Server-Zertifikat mit Zertifikatskette.
  Das Internet-Gateway bestätigt den Fingerabdruck und das Site-Zertifikat. Das Site-Zertifikat wird verwendet, um zum zum ersten Mal eine Verbindung zum Gateway herzustellen. Das Site-Zertifikat ist wesentlich, da es verwendet wird, um eine permanente Clientzertifikatanfrage zu generieren.
- Liste der Internet-Gateways, die dem Cloud-fähigen Agent zur Verfügung stehen.
- Ressourcenziel, dem der Computer automatisch hinzugefügt wird.
- Organisationsgruppe, der der Computer automatisch hinzugefügt wird.
- Skripts, mit denen der Symantec Management-Agent so konfiguriert werden kann, dass er die angegebenen Einstellungen verwendet.

Warnung: Das Symantec Management-Agent-Installationspaket ist für einen begrenzten Zeitraum (standardmäßig sieben Tage) ab dem Zeitpunkt der Generierung gültig. Das temporäre Site-Zertifikat, das im Paket enthalten ist, läuft nach dieser Zeit ab. Wenn Sie das Paket verwenden, nachdem sein Site-Zertifikat abgelaufen ist, kann der installierte Agent das Internet-Gateway für die Kommunikation nicht verwenden. Sie müssen den Agent erneut installieren und dabei ein neu generiertes Installationspaket verwenden, das ein gültiges Site-Zertifikat enthält.

---

6. Klicken Sie im Dialogfeld "Dateidownload" auf "Speichern" und geben Sie dann den gewünschten Speicherort für die Datei an.
7. Wenn das Paket vollständig heruntergeladen ist, klicken Sie auf "Schließen".
8. Klicken Sie im Dialogfeld "Installationspaket für den Cloud-fähigen Agent" auf "Schließen".
9. Legen Sie das Symantec Management-Agent-Installationspaket auf dem entsprechenden nicht verbundenen Computer ab.

10 Führen Sie das Agent-Installationspaket auf dem nicht verbundenen Computer aus.

Das Agent-Paket ist eine selbstextrahierende, ausführbare Datei und die Installation wird ohne Meldungsausgabe ausgeführt.

Nach der Installation konfiguriert sich Symantec Management Agent automatisch und führt folgende Schritte durch:

- Der Agent handelt sein Zertifikat neu aus.
  Der Agent fordert vom Notification Server ein neues Zertifikat an und erhält dieses: Das neue Zertifikat ist speziell diesem Clientcomputer zugeordnet und ersetzt das vorübergehende Site-Zertifikat, das im Installationspaket des Agent enthalten war.
- Der Agent wird den entsprechenden Ressourcenzielen und Organisationsgruppen auf der Symantec Management-Plattform zugewiesen.

11 Überprüfen Sie, ob die Installation erfolgreich war. Sie können die Symantec Management Console verwenden, um anhand der Berichte zu prüfen, ob der neu verwaltete Computer vorhanden ist.

Wenn Sie im Installationspaket eine Organisationsgruppe angegeben haben, können Sie außerdem prüfen, ob der neue Computer zur entsprechenden Gruppe hinzugefügt wurde.

Siehe "Anzeigen von Berichten der Cloud-fähigen Verwaltung" auf Seite 353.

Eine detaillierte Beschreibung des Prozesses zum Einrichten der Cloud-fähigen Verwaltung finden Sie unter Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

Kapitel 21

Ausführen von Aufgaben in der Cloud-fähigen Verwaltung

In diesem Kapitel werden folgende Themen behandelt:

- Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung

Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung

In diesem Abschnitt werden einige Fehlerbehebungs- und Wartungsaufgaben beschrieben, die Sie möglicherweise durchführen müssen.

Siehe "Info zu Cloud-fähiger Verwaltung" auf Seite 297.

Tabelle 21-1 Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung

Aufgabe	Beschreibung
Anwenden einer Stammzertifizierungsstelle auf einen verwalteten Computer	Bevor Sie einen direkt verwalteten Computer auf Cloud-fähige Verwaltung migrieren können, müssen Sie sicherstellen, dass der Agent über HTTPS mit dem Notification Server kommunizieren kann. Der Agent muss dem Notification Server vertrauen, damit HTTPS für die Kommunikation verwendet werden kann. Bei Bedarf können Sie auf dem verwalteten Computer unter "Vertrauenswürdige Stammzertifizierungsstellen" eine Stammzertifizierungsstelle (CA) hinzufügen. Siehe "Anwenden eines Zertifikats einer Stammzertifizierungsstelle auf einen verwalteten Computer" auf Seite 305.

Aufgabe	Beschreibung
Generieren eines temporären Clientzertifikats	Die Cloud-fähige Verwaltung weist verwalteten Computern und Site Servern Clientzertifikate zu, damit sie sich beim Notification Server identifizieren können. Sie müssen möglicherweise ein temporäres Clientzertifikat für einen verwalteten Computer generieren. Ein Tool zum Generieren des Clientzertifikats (`AeXGenClientCert.exe`) steht auf dem Notification Server zur Verfügung. Siehe "Generieren eines temporären Clientzertifikats" auf Seite 343.
Installieren eines temporären Clientzertifikats auf einem verwalteten Computer	Wenn der Symantec Management-Agent die Kommunikation über die Internet-Gateways beendet, ist sein Zertifikat möglicherweise beschädigt. Sie können die Kommunikation wiederherstellen, indem Sie ein temporäres Clientzertifikat auf dem entsprechenden verwalteten Computer installieren. Der Symantec Management-Agent verwendet das temporäre Zertifikat, um die Verbindung zu den Internet-Gateways zu reparieren. Sie können bei Bedarf Zertifikate dem Zertifikatspeicher des Agent-Diensts hinzufügen oder daraus entfernen. Siehe "Installieren eines temporären Zertifikats auf einem verwalteten Computer" auf Seite 346.
Sperren eines Clientzertifikats auf einem verwalteten Computer	Wenn Sie glauben, dass ein bestimmtes Clientzertifikat kompromittiert wurde und nicht mehr vertrauenswürdig ist, können Sie das Zertifikat sperren. Wenn beispielsweise ein Cloud-fähiger Laptop verloren geht oder gestohlen wird, müssen Sie sein Zertifikat sofort widerrufen. Die Aufhebung des Zertifikats verhindert, dass der verwaltete Computer im Cloud-fähigen Modus auf Ihr Netzwerk zugreift. Siehe "Widerrufen eines Zertifikats der Cloud-fähigen Verwaltung" auf Seite 347.
Erzwingen der Verwendung eines bestimmten Internet-Gateways durch einen Cloud-fähigen Agent	Wenn der Agent keine gültige Liste mit Internet-Gateways hat, können Sie ihn zwingen, über bestimmte Gateways zu kommunizieren. Sie können bei Bedarf Internet-Gateways zur Liste hinzufügen oder daraus entfernen. Siehe "Erzwingen, dass der Symantec Management-Agent ein angegebenes Gateway verwendet" auf Seite 350.
Sichern und Wiederherstellen des Internet-Gateways	Sie können Ihre Internet-Gateway-Einstellungen sichern und im Falle eines Fehlers ihren ursprünglichen Zustand wiederherstellen. Siehe "Sichern und Wiederherstellen eines Internet-Gateways" auf Seite 351.
Anzeigen von Berichten der Cloud-fähige Verwaltung	Ein Satz vordefinierte Berichte wird zur Verfügung gestellt, um Ihnen zu helfen, Ihre Cloud-fähigen Computer zu überwachen und zu verwalten. Siehe "Anzeigen von Berichten der Cloud-fähigen Verwaltung" auf Seite 353.

Generieren eines temporären Clientzertifikats

Die Cloud-fähige Verwaltung weist verwalteten Computern und Site Servern Clientzertifikate zu, damit sie sich beim Notification Server identifizieren können.

Mithilfe des Tools zum Generieren von Clientzertifikaten (`AeXGenClientCert.exe`) können Sie die erforderlichen Clientzertifikate erstellen. Die Zertifizierungsstelle (CA) des Notification Server-Agent stellt diese Zertifikate aus. Der öffentliche Teil des Zertifikats wird in der Configuration Management Database gespeichert (CMDB). Sowohl der öffentliche als auch der private Teil werden einer PKCS#12 (PFX)-Datei hinzugefügt.

Hinweis: Das generierte Zertifikat ist für einen begrenzten Zeitraum gültig. Standardmäßig beträgt dieser Zeitraum sieben Tage, aber Sie können dies bei Bedarf ändern.

Sie müssen möglicherweise ein temporäres Zertifikat für einen verwalteten Computer generieren. In diesem Fall müssen Sie die entsprechende PFX-Datei generieren und dann die Datei auf dem verwalteten Computer oder dem Site Server installieren.

So generieren Sie ein Clientzertifikat

- Öffnen Sie auf dem Notification Server-Computer ein Befehlsfenster und führen Sie dann die folgende Kommandozeile mit den entsprechenden Parametern aus:

  ```
  \Programme\Altiris\Notification Server\bin\Tools\AeXGenClientCert
  <AllgemeinerName> [-o Zertifikat.pfx] [-p Kennwort]
  ```

AllgemeinerName	Die ID, die Sie in der Betreffzeile des Zertifikats anzeigen möchten. Diese ID wird für Berichts- und Diagnosezwecke verwendet. Diese Kennung sollte mit dem Parameter "Installationsname" übereinstimmen, der im Installationspaket des Symantec Management-Agent angegeben wurde. Siehe "Parameter für Installationspakete Cloud-fähiger Agents" auf Seite 544.
Zertifikat.pfx	Der vollständige Pfad und Name der PFX-Datei, die Sie generieren möchten. Wenn Sie diesen Parameter auslassen, wird das generierte Zertifikat im lokalen Verzeichnis gespeichert. Die Zertifikatsdatei wird nach dem angegebenen allgemeinen Namen benannt und mit der Erweiterung ".pfx" versehen (***AllgemeinerName.pfx***).
Kennwort	Das Kennwort, das Sie verwenden möchten. Wenn Sie diesen Parameter auslassen, ist das Kennwort leer. Es wird kein Standardkennwort angewendet.

  Name und Pfad der generierten Datei werden im Befehlsfenster angezeigt.

  Sie müssen die generierte Zertifikatsdatei auf geeignete Medien kopieren und im Stammordner des entsprechenden Clientcomputers ablegen. Anschließend müssen Sie auf dem Clientcomputer den Kommandozeilenschalter `/importcert` verwenden, damit der Symantec Management-Agent das neue Zertifikat verwendet.

  Siehe "Installieren eines temporären Zertifikats auf einem verwalteten Computer" auf Seite 346.

Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Installieren eines temporären Zertifikats auf einem verwalteten Computer

Wenn der Symantec Management-Agent die Kommunikation über die Internet-Gateways beendet, ist sein Zertifikat möglicherweise beschädigt. Sie können dieses Problem beheben, indem Sie ein temporäres Zertifikat auf dem entsprechenden Clientcomputer installieren.

Der Symantec Management-Agent verwendet das temporäre Zertifikat, um über das entsprechende Internet-Gateway eine Verbindung zum Notification Server herzustellen. Er fordert dann ein neues Zertifikat an, das für diesen Computer eindeutig ist.

Die Zertifikatsdatei muss einen privaten Schlüssel ohne zugeordnetes Kennwort enthalten.

So installieren Sie temporäre Zertifikate auf einem verwalteten Computer

1. Generieren Sie das temporäre Clientzertifikat *tempcert.pfx*.

   Sie können mithilfe eines Kommandozeilenprogramms auf dem Notification Server-Computer ein temporäres Clientzertifikat generieren. Das Kommandozeilenprogramm generiert eine PFX-Datei, die das Zertifikat und den privaten Schlüssel enthält.

   Siehe "Kommandozeilenprogramme des Notification Servers" auf Seite 538.

   Hinweis: Standardmäßig hat die generierte Datei kein Kennwort. Geben Sie kein Kennwort an, da der Symantec Management-Agent kennwortgeschützte PFX-Dateien nicht verwenden kann.

   Siehe "Generieren eines temporären Clientzertifikats" auf Seite 343.

2. Legen Sie die generierte PFX-Datei im Stammordner auf dem verwalteten Computer ab.

3. Öffnen Sie ein Befehlsfenster und führen Sie die folgende Kommandozeile aus:

   ```
   [Agent-Installationsordner]\AeXNSAgent.exe
   /importcert=tempcert.pfx
   ```

   Beispiel:

   \Programme\Altiris\Altiris Agent\AeXNSAgent.exe /importcert=myRootCert.pfx

4. Starten Sie den Symantec Management-Agent neu, um die neuen Einstellungen wirksam werden zu lassen.

So entfernen Sie ein Zertifikat von einem verwalteten Computer

- Öffnen Sie auf dem verwalteten Computer ein Befehlsfenster und führen Sie die folgende Kommandozeile aus:

  ```
  [Agent-Installationsordner]\AeXNSAgent.exe /removecert
  ```

  Dieser Befehl entfernt das aktuelle Zertifikat vom Symantec Management-Agent.

  Beispiel:

  \Programme\Altiris\Altiris Agent\AeXNSAgent.exe /removecert

Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Siehe "Kommandozeilen-Switches für Cloud-fähige Agents" auf Seite 545.

Widerrufen eines Zertifikats der Cloud-fähigen Verwaltung

Durch Widerrufen eines Zertifikats der Cloud-fähigen Verwaltung (CEM-Zertifikat) wird verhindert, dass der verwaltete Computer im Cloud-fähigen Modus auf Ihr Netzwerk zugreift. Wenn beispielsweise ein Cloud-fähiger Laptop verloren geht oder gestohlen wird, müssen Sie sein Zertifikat sofort widerrufen.

Der Agent hat zwei CEM-Zertifikate. Mit dem einen Zertifikat stellt der Agent eine Verbindung zum Internet-Gateway her und mit dem anderen zum Notification Server. Wenn das Zertifikat, mit dem der Agent eine Verbindung zum Notification Server herstellt, widerrufen wird, lehnt der Notification Server Verbindungsversuche von einem solchem Client ab. Das Internet-Gateway kann jedoch direkt vom Notification Server keine Informationen über widerrufene Zertifikate erhalten. Um ein bestimmtes Zertifikat auf dem Internet-Gateway zu widerrufen, müssen Sie der Zertifikatswiderrufsliste (CRL) auf dem Notification Server die Zertifikatdetails hinzufügen, eine aktualisierte CRL-Datei generieren und dann die aktualisierte CRL-Datei auf das entsprechende Internet-Gateway anwenden.

Hinweis: Sie müssen die aktualisierte CRL-Datei auf jedes Internet-Gateway anwenden, das der widerrufene Agent möglicherweise verwendet.

Beachten Sie, dass durch das Widerrufen des Cloud-fähigen Zertifikats der Zugriff des verwalteten Computer auf den Notification Server nur dann blockiert wird, wenn sich der Computer im Cloud-fähigen Modus befindet. Wenn das Vertrauen des Agent nicht widerrufen wird, kann er weiterhin im lokalen Modus arbeiten.

So widerrufen Sie ein Zertifikat der Cloud-fähigen Verwaltung

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Erweitern Sie im linken Teilfenster unter "Berichte" "Notification Server-Verwaltung > Zertifikate" und klicken Sie dann auf "Zertifikat nach Fingerabdruck".
3. Klicken Sie auf auf der Berichtseite "Zertifikat nach Fingerabdruck" mit der rechten Maustaste auf das Zertifikat, das Sie widerrufen möchten, und klicken Sie dann auf "Zertifikat widerrufen".

   Wenn Sie das Zertifikat auf der Berichtseite "Zertifikat nach Fingerabdruck" widerrufen, werden die Zertifikatdetails der CRL-Datei automatisch hinzugefügt.

   Die CRL wird im Stammcomputerspeicher gespeichert, obwohl die Zertifikate in der Configuration Management Database (CMDB) gespeichert werden. Das Tool zum Widerrufen von Zertifikaten (`AeXRevokeCertificate.exe`) lädt zuerst die bestehende CRL, sofern vorhanden. Wenn im Zertifikatspeicher keine CRL vorhanden ist, erstellt das Tool eine. Anschließend fügt das Tool die Seriennummer des Zertifikats der Liste hinzu und generiert eine PEM-kodierte Datei mit der aktualisierten CRL. Sie müssen dann die generierte CRL-Datei auf dem Internet-Gateway-Computer ablegen und ein Skript ausführen, um die aktualisierte Liste auf das Internet-Gateway anzuwenden.

   Standardmäßig befindet sich die CRL-Datei an folgenden Speicherort auf dem Notification Server:

   ```
   \Programme\Altiris\Notification
   Server\bin\Tools\AeXRevokeCertificate\EMEncodedFile.CRL
   ```

So fügen Sie ein Zertifikat der Cloud-fähigen Verwaltung der CRL manuell hinzu

1. Rufen Sie die Seriennummer und den Fingerabdruck des Clientzertifikats ab, das Sie widerrufen möchten.

   Wenn Sie Zugriff auf den Clientcomputer haben, können Sie die Microsoft Management Console (MMC) verwenden, um die Details des Clientzertifikats zu suchen.

   Wenn Sie keinen Zugriff auf den Clientcomputer haben, können Sie eine der folgenden Methoden verwenden:

   - Öffnen Sie in der Symantec Management Console den Ressourcenmanager und zeigen Sie die Grundinventarinformationen zum Clientcomputer an. Der Menüpfad lautet "Ansicht" > "Datenklassen" > "Inventar" > "Grundinventar" > "AeX AC-Zertifikat". Die gesamten Details des Clientzertifikats werden angezeigt, einschließlich Seriennummer und Fingerabdruck.

- Suchen Sie in der CMDB der Symantec Management-Plattform, indem Sie eine SQL-Abfrage ausführen. Die Clientzertifikate werden in der Tabelle "CertificateRegistration" gespeichert.
- Öffnen Sie auf dem Internet-Gateway die Zugriffsprotokolldatei und suchen Sie nach einem Eintrag zu dem Client. Die Datei "access.log" wird im Internet-Gateway-Installationsordner im Ordner "Apache\logs" gespeichert. Jeder Eintrag in der Protokolldatei enthält den Namen des Computers, der auf das Internet-Gateway zugegriffen hat, und die entsprechende Zertifikatsseriennummer.

2 Öffnen Sie auf dem Notification Server-Computer ein Befehlsfenster und führen Sie dann die folgende Kommandozeile mit den entsprechenden Parametern aus:

```
\Programme\Altiris\Notification
Server\bin\Tools\AeXRevokeCertificate -o <PEMEncodedFile.CRL> <-t
SHA-1-Fingerabdruck | -s Seriennummer>
```

PEM-kodierteDatei.CRL	Der vollständige Pfad und Name der PEM-kodierten CRL-Datei, die Sie generieren möchten. Wenn Sie diesen Parameter auslassen, wird die generierte Datei im lokalen Verzeichnis gespeichert.
SHA-1-Fingerabdruck	Die eindeutige ID des Zertifikats.
Seriennummer	Wenn sich mehr als ein Zertifikat mit der gleichen Seriennummer in der Datenbank befindet, verwenden Sie einen SHA-1-Fingerabdruck, um das Zertifikat zu identifizieren. Umgekehrt gilt: Wenn zwei Zertifikate denselben Fingerabdruck haben, identifizieren Sie das Zertifikat durch die Seriennummer. **Hinweis:** An einigen Stellen werden Fingerabdruck und Seriennummer möglicherweise als durch Leerzeichen getrennte Oktetts angezeigt. Wenn Sie sie jedoch als Kommandozeilenparameter angeben, dürfen sie keine Leerzeichen enthalten.

Die aktualisierte CRL-Datei wird generiert.

So wenden Sie die CRL auf ein Internet-Gateway an

1. Legen Sie die generierte CRL auf dem Internet-Gateway-Computer an folgendem Ort ab:

   `[Installationsordner des SMP-Internet-Gateway]\Apache\certs\crl`

   Der Standardinstallationsordner ist `\Programme x86\Symantec\SMP Internet Gateway`. Der Pfad hängt jedoch vom Verzeichnis ab, das während der Installation des Internet-Gateway angegeben wurde.

2. Doppelklicken Sie im gleichen Ordner auf "UpdateCrlHashes.cmd", um das Skript "Update CRL" auszuführen.

   Dieses Skript führt die notwendige Konfiguration durch und startet dann das Internet-Gateway neu, damit die Änderungen in Kraft treten.

Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Erzwingen, dass der Symantec Management-Agent ein angegebenes Gateway verwendet

Wenn der Agent keine gültige Liste mit Internet-Gateways hat, können Sie ihn zwingen, über bestimmte Gateways zu kommunizieren. Sie erzwingen eine bestimmte Liste mit Gateways von der Kommandozeile aus oder durch eine Änderung der Registrierungseinstellungen. Eine Kommandozeile steht für das Hinzufügen einzelner Gateways zur Verfügung.

Wenn Sie ein Internet-Gateway aus der Symantec Management-Agent-Konfiguration entfernen möchten, können Sie dies durch Bearbeiten der Registrierung tun.

Details zu Internet-Gateways werden in der Registrierung gespeichert. Sie können Internet-Gateways hinzufügen oder entfernen, indem Sie die Einträge unter dem folgenden Schlüssel bearbeiten:

`HKEY_LOCAL_MACHINE\SOFTWARE\Altiris\Communications\Secure Gateways`

Jedes Internet-Gateway hat eine Reihe von Werten unter dem Schlüssel `<GatewayName>`.

Hinweis: Sie müssen den Symantec Management-Agent neu starten, damit diese Einstellungen in Kraft treten.

So erzwingen Sie, dass der Symantec Management-Agent ein angegebenes Internet-Gateway verwendet

- Öffnen Sie auf dem Clientcomputer ein Befehlsfenster und führen Sie die folgende Kommandozeile aus:

  ```
  \Programme\Altiris\Altiris Agent\AeXNSAgent.exe
  /gw=gatewayName,port,thumbprint
  ```

gatewayName	Der Name oder die IP-Adresse des Gateway-Computers.
Port	Die Portnummer, die der Symantec Management-Agent verwenden muss, um eine Verbindung mit dem Gateway herstellen zu können. Der Standard-Port ist 443.
thumbprint	Der Zertifikatsfingerabdruck des Zertifikats, das das Gateway für sichere Verbindungen verwendet. **Hinweis:** Stellenweise wird der Fingerabdruck möglicherweise als durch Leerzeichen getrennte Byte angezeigt. Wenn Sie ihn jedoch als Kommandozeilenparameter angeben, darf er keine Leerzeichen enthalten.

  Jeder Parameter muss durch ein Komma getrennt sein. Es sind keine Leerzeichen oder sonstige Satzzeichen zulässig.

  Beispiel:

  \Programme\Altiris\Altiris Agent\AeXNSAgent.exe /gw=myGateWay.symantec.com,443,0f8753ef3da6bc4

Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Siehe "Kommandozeilen-Switches für Cloud-fähige Agents" auf Seite 545.

Sichern und Wiederherstellen eines Internet-Gateways

Durch Sichern Ihres Internet-Gateways können Sie bei Ausfällen seinen ursprünglichen Zustand wiederherstellen. Sie können eine teilweise Wiederherstellung durchführen, wenn einige Dateien aus der Backup-Liste fehlen oder beschädigt sind. Sie können bei schwerwiegender Beschädigung der Internet-Gateway-Konfiguration auch eine vollständige Wiederherstellung durchführen. Beispiel: Sie haben eine Festplatte auf Ihrem Internet-Gateway-Computer ausgetauscht.

Sie können ein Backup durchführen, ohne den Internet-Gateway-Dienst zu beenden.

Sie sollten die Dateien in den angegebenen Ordnern wie folgt sichern:

- Die Dateien `openssl.cnf`, `server.crt` und `server.key` im Ordner `C:\\Programme\Symantec\SMP Internet Gateway\Apache\certs`
- Alle Dateien im Ordner `C:\\Programme\Symantec\SMP Internet Gateway\Apache\certs\client`
- Alle Dateien im Ordner `C:\\Programme\Symantec\SMP Internet Gateway\Apache\certs\crl`
- Alle Dateien im Ordner `C:\\Programme\Symantec\SMP Internet Gateway\Apache\conf`

So führen Sie eine teilweise Wiederherstellung durch

1. Öffnen Sie den Internet-Gateway-Manager der Symantec Management-Plattform und klicken Sie auf der Registerkarte "Allgemein" unter "Internet-Gateway-Dienst" auf "Stopp", um den Internet-Gateway-Dienst anzuhalten.
2. Stellen Sie Problemelemente aus der Backup-Liste wieder her.
3. Klicken Sie im Internet-Gateway-Manager der Symantec Management-Plattform auf der Registerkarte "Allgemein" unter "Internet-Gateway-Dienst" auf "Starten", um den Internet-Gateway-Dienst zu starten.

   Vergewissern Sie sich nach dem Starten des Dienstes, ob die Internet-Gateway-Einstellungen korrekt sind und alles richtig funktioniert.

So führen Sie eine vollständige Wiederherstellung durch

1. Führen Sie eine Neuinstallation des Internet-Gateways durch.

   Deaktivieren Sie am Ende der Installation die Option "Konfigurationsassistenten starten".
2. Stellen Sie alle Elemente aus der Backup-Liste an den entsprechenden Speicherorten auf dem Internet-Gateway-Computer wieder her.
3. Öffnen Sie den Internet-Gateway-Manager der Symantec Management-Plattform und klicken Sie auf der Registerkarte "Einstellungen" auf "Assistenten ausführen".
4. Blättern Sie durch die Seiten des Assistenten Internet-Gateway-Konfiguration der Symantec Management-Plattform und stellen Sie sicher, dass alle Daten korrekt im voraus befüllt sind.

5 Geben Sie auf der Seite "Benutzerkonto" die Identifikationsdaten für den Internet-Gateway-Dienst an.

6 Überprüfen Sie auf der Seite "Übersicht" die Einstellungen, und stellen Sie sicher, dass die Option "Dienste automatisch neu starten?" aktiviert ist. Klicken Sie anschließend auf "Fertig stellen".

   Vergewissern Sie sich nach dem Starten des Dienstes, ob die Internet-Gateway-Einstellungen korrekt sind und alles richtig funktioniert.

Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Anzeigen von Berichten der Cloud-fähigen Verwaltung

Ein umfassender Satz von Berichten wird Ihnen zur Verfügung gestellt, um Sie bei der Überwachung und Verwaltung Ihrer Cloud-fähigen Computer zu unterstützen. Sie können benutzerdefinierte Berichte auch Ihren Anforderungen entsprechend erstellen.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

So zeigen Sie Berichte der Cloud-fähigen Verwaltung an

1 Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".

2 Wählen Sie im linken Teilfenster die Optionsfolge "Berichte > Notification Server-Verwaltung > Agent > Cloud-fähige Verwaltung" und klicken Sie anschließend auf den Bericht, den Sie anzeigen möchten.

Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Abschnitt 6

Verwalten von Symantec Management-Plattform-Ressourcen

- Kapitel 22. Konfigurieren der Ressourcensicherheit
- Kapitel 23. Konfigurieren der Ressourcenfilter und -ziele
- Kapitel 24. Konfigurieren von Paketen
- Kapitel 25. Verwenden von Richtlinien
- Kapitel 26. Verwenden von Aufgaben und Aufträgen
- Kapitel 27. Verwenden des Ressourcenmanagers
- Kapitel 28. Verwenden von Notification Server-Berichten
- Kapitel 29. Erstellen benutzerdefinierter Notification Server-Berichte
- Kapitel 30. Anzeigen von Ressourceninformationen

Kapitel 22

Konfigurieren der Ressourcensicherheit

In diesem Kapitel werden folgende Themen behandelt:

- Konfigurieren der Ressourcensicherheit
- Überlegungen zu Ressourcen mit Bereichsfestlegung

Konfigurieren der Ressourcensicherheit

Das Ressourcensicherheitmodell hat sich erheblich für Notification Server 7.0 geändert. Ressourcen, die alle Computer, Benutzer und alles andere enthält, das in CMDB oder im Ressourcenmodell definiert wird, beziehen jetzt alle ihre Berechtigungsbewilligungen aus den Organisationsansichten und aus den Gruppen, zu denen sie gehören. Dies ersetzt die Implementierung des Notification Servers 6.0, bei der das Sichern von Standardsammlungen und von Ressourcenordnern notwendig war.

Hinweis: Es gibt einige Ausnahmen, wie zum Beispiel Pakete, die Ressourcen sind, die aber auch Elemente sind, die in der Symantec Management Console-Ordnerstruktur angezeigt werden. Die Sicherheitsoptionen für diese Elemente werden in der Ordnerstruktur deaktiviert. Sicherheit dafür wird auf die gleiche Art wie für andere Ressourcen eingestellt.

Eine Organisationsansicht ist eine hierarchische Ressourcengruppe (Organisationsgruppe), die einer tatsächlichen Struktur oder Ansicht Ihres Unternehmens entspricht. So können Sie zum Beispiel Organisationspübersichten erstellen, die Ihre Ressourcen nach geografischem Standort, Abteilung oder Netzwerkstruktur gruppieren. Genau wie in der tatsächlichen Umgebung kann eine

Ressource vielleicht nur einmal in einer Organisationsübersicht erscheinen (muss aber nicht).

Die Zuweisung von Ressourcen in Organisationsgruppen läuft automatisch ab und Sie können sie nicht ändern. Beachten Sie, dass es möglicherweise eine Verzögerung zwischen den Ressourcen gibt, die erkannt werden und denen, die in der entsprechenden Organisationsgruppe angezeigt werden. Jede neu erkannte Ressource wird in die Organisationsgruppe der höchsten Ebene platziert und verbleibt dort, bis sie in die entsprechende Organisationsgruppe verschoben wird, wenn der Organisationsansicht-Aktualisierungszeitplan ausgeführt wird.

Sie können Ressourcen aus einer beliebigen Organisationsansicht entfernen, außer der Standardansicht. Wenn eine Ressource aus der CMDB gelöscht wird, wird sie automatisch aus allen Organisationsansichten entsprechend dem Delta-Aktualisierungszeitplan entfernt.

Siehe "Planen von Ressourcen-Mitgliedschaftsaktualisierungen" auf Seite 384.

Sie richten Sicherheit ein, indem Sie die entsprechenden Berechtigungen für jede Sicherheitsrolle auf jeder Organisationsansicht und auf den Organisationsgruppen innerhalb jeder Ansicht zuweisen. Eine Berechtigung, die einer Organisationsgruppe zugewiesen wird, trifft auf alle Ressourcen in dieser Gruppe zu und gilt standardmäßig für alle ihre untergeordneten Gruppen. Sie können Berechtigungen nicht direkt einer bestimmten Ressource zuweisen.

Berechtigungsbewilligungen auf einer Ressource werden über Organisationsansichten akkumuliert. Die Berechtigungen, die eine Sicherheitsrolle auf einer bestimmten Ressource hat, ist die Gesamtmenge aller Berechtigungen, denen die Ressource durch die Organisationsgruppen, zu denen sie gehört, zugewiesen worden ist. Wenn eine Sicherheitsrolle über Berechtigungen zum Durchführen einer Aktion auf einer Ressource in einer Organisationsansicht verfügt, kann die Rolle diese Aktion unabhängig davon durchführen, ob die Berechtigung auf anderen Organisationsansichten, die die gleiche Ressource enthalten, angewendet wird. Wenn eine Sicherheitsrolle beispielsweise über Lesezugriff für eine Ressource in einer Organisationsansicht verfügt, über Schreibzugriff für dieselbe Ressource in einer anderen Organisationsansicht, aber über keinen Zugriff auf die Ressource in einer dritten Organisationsansicht verfügt, verfügt die Rolle über Lese- und Schreibzugriff für die Ressource.

Das Implementieren von Ressourcensicherheit gibt jeder Sicherheitsrolle ihre eigene eindeutige Ansicht oder "Bereich" der verfügbaren Ressourcen. Die Sicherheitsrolle legt fest, auf welche Ressourcen ihre Mitglieder zugreifen können und welche Aktionen sie daran ausführen können. Filter, Ziele und Berichtergebnisse sind dynamisch und werden entsprechend der Rolle des Benutzers, automatisch festgelegt. Deshalb enthalten Filter, Ziele und Berichtergebnisse immer nur die Ressourcen, zu denen dieser Benutzer die notwendigen Zugriffsberechtigungen hat.

Konfigurieren von Ressourcensicherheit ist ein optionaler Schritt beim Einrichten von Symantec Management Plattform-Sicherheit.

Siehe "Einrichten der Sicherheit für die Symantec Management-Plattform" auf Seite 88.

Hinweis: Wenn ein Ziel ausgewertet wird, sind nur die Ressourcen, auf die der Benutzer Lesezugriff hat, verfügbar. Infolgedessen ist die einzige Sicherheitsberechtigung, die ein Benutzer benötigt, um eine Aufgabe oder eine Richtlinie auf eine Ressource anzuwenden, die Leseberechtigung auf der Ressource.

Tabelle 22-1 Konfigurieren der Ressourcensicherheit

Schritt	Aktion	Beschreibung
Schritt 1	Identifizieren Sie Ihre Anforderungen an die Ressourcenverwaltung und -sicherheit.	Sie müssen Ihre Anforderungen an die Ressourcenverwaltung und -sicherheit bestimmen und die Organisationsansichtstrukturen planen, die Ihre Anforderungen am besten erfüllen. Sie können jede beliebige Struktur verwenden. Beispielsweise können Sie Organisationsansichten verwenden, die auf Geografie, Unternehmensfunktion oder Verwaltungsstruktur basieren. Weitere Informationen finden Sie im *Implementierungs- und Planungshandbuch für IT Management Suite*.
Schritt 2	Erstellen Sie die gewünschten Organisationsansichten.	Erstellen Sie die Organisationsansichten, die Sie benötigen, um die entsprechenden logischen Strukturen in Ihrer Organisation zu errichten. Siehe "Erstellen und Konfigurieren einer Organisationsansicht" auf Seite 358. Siehe "Erstellen und auffüllen einer Organisationsansicht oder eine Gruppe" auf Seite 359.
Schritt 3	Unter jeder Organisationsansicht erstellen Sie die gewünschten Organisationsgruppen und weisen ihnen die gewünschten Ressourcen zu.	Innerhalb jeder Organisationsansicht können Sie eine Hierarchie von Gruppen erstellen, um die gewünschte Organisationsstruktur darzustellen. Neue Ressourcen werden automatisch der Organisationsansicht "Standard" hinzugefügt. Sie können sie in eine entsprechende Gruppe Ihrer Organisationsansichten verschieben. Siehe "Erstellen und Konfigurieren von Organisationsgruppen" auf Seite 360. Siehe "Anzeigen von Ressourcen in einer Organisationsgruppe" auf Seite 361.

Schritt	Aktion	Beschreibung
Schritt 4	Weisen Sie die entsprechenden Sicherheitsrollen jeder Organisationsgruppe zu.	Durch das Zuweisen einer Sicherheitsrolle zu einer Organisationsgruppe erhalten Benutzer mit dieser Rolle Zugriff auf alle Ressourcen, die direkt in dieser Gruppe enthalten sind. Sie müssen die Berechtigungen angeben, die jede Rolle für die Gruppe besitzt. Standardmäßig gelten Sicherheitseinstellungen für eine Gruppe auch für alle untergeordneten Gruppen. Bei Bedarf können Sie diese Vererbung unterbrechen. Siehe "Festlegen der Sicherheit für eine Organisationsgruppe" auf Seite 362.

Erstellen und Konfigurieren einer Organisationsansicht

Eine Organisationsansicht ist eine hierarchische Ressourcengruppe (Organisationsgruppe), die einer tatsächlichen Struktur oder Ansicht Ihres Unternehmens entspricht. So können Sie zum Beispiel Organisationspübersichten erstellen, die Ihre Ressourcen nach geografischem Standort, Abteilung oder Netzwerkstruktur gruppieren. Genau wie in der tatsächlichen Umgebung kann eine Ressource vielleicht nur einmal in einer Organisationsübersicht erscheinen (muss aber nicht).

Organisationsansichten sind eine sichere Methode zur Unterteilung von Ressourcen in deutlich strukturierte und einfach verwaltbare Einheiten. Die Organisationsübersicht kann keine Ressourcen direkt enthalten. Alle Ressourcen müssen in Organisationsgruppen abgelegt werden. Sie können Organisationsübersichten und -gruppen für eine Vielzahl von Organisationsanforderungen nutzen. Sie können Ihre Organisationsübersichten mit Hilfe des vertrauten NT-Sicherheitsvererbungsmodells schützen, das in der gesamten Symantec Management-Plattform verwendet wird.

Sie können Organisationsansichten und Gruppen innerhalb von Zielen verwenden, wenn Sie eine Richtlinie oder Aufgabe auf ausgewählte Computer, Benutzer oder Ressourcen anwenden möchten. Die Organisationsübersicht oder -gruppe wird genau wie ein Filter verwendet, umfasst aber die nötige Sicherheit, um zu gewährleisten, dass nur die Ressourcen enthalten sind, für die der Besitzer des Ziels Berechtigungen hat.

Diese Aufgabe ist ein Schritt beim Konfigurieren der Ressourcensicherheit.

Siehe "Konfigurieren der Ressourcensicherheit" auf Seite 355.

So erstellen Sie eine Organisationsgruppe

1. Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Organisationsansichten und Gruppen".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner "Organisationsansichten" und wählen Sie im Kontextmenü die Option "Neu > Organisationsansicht".
3. (Optional) Bearbeiten Sie im rechten Teilfenster den Namen und die Beschreibung der Organisationsansicht.
4. So geben Sie die die anzuzeigenden Organisationsgruppen an
   - Klicken Sie im rechten Teilfenster auf "Filter".
   - Aktivieren Sie im Dialogfeld "Angezeigte Gruppen filtern" das Kontrollkästchen neben den Organisationsgruppen, die für diese Organisationsansicht sichtbar sein sollen, und klicken Sie dann auf "OK".

Erstellen und auffüllen einer Organisationsansicht oder eine Gruppe

In der erweiterten Ansicht "Computer" können Sie Organisationsansichten und Gruppen leicht erstellen und auffüllen.

So erstellen oder füllen Sie eine Organisationsansicht oder eine Gruppe auf

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Computer".
2. Klicken Sie mit der rechten Maustaste auf "Alle Computeransichten" und klicken Sie dann auf "Neu > Organisationsansicht".
3. Geben Sie im Dialogfeld "Organisationsansicht" den Namen für die Organisationsansicht ein und klicken Sie dann auf "OK".
4. Klicken Sie mit der rechten Maustaste auf die neue Organisationsansicht, und klicken Sie auf "Neu > Organisationsgruppe".

   Beachten Sie, dass Sie Organisationsgruppen nicht der Standard-Organisationsansicht "Alle Computer" hinzufügen können.
5. Geben Sie im Dialogfeld "Organisationsgruppe" den Namen für die neue Gruppe ein und klicken Sie dann auf "OK".
6. Um die neue Organisationsgruppe aufzufüllen, führen Sie folgende Schritte durch:
   - Klicken Sie unter "Alle Computeransichten" auf "Alle Computer".
   - Im Listenbereich wählen Sie die Computer aus, die Sie dieser Organisationsgruppe hinzufügen möchten.

Sie können die Tasten "Shift" oder "Strg" verwenden, um mehrere Computer auszuwählen.

- Ziehen Sie die ausgewählten Computer auf die neue Organisationsgruppe oder klicken Sie mit der rechten Maustaste auf einen der ausgewählten Computer und klicken Sie dann auf "Einer Organisationsgruppe hinzufügen". Klicken Sie im Dialogfeld "Einer Organisationsgruppe hinzufügen" auf die Gruppe, der Sie die Computer hinzufügen möchten, und klicken Sie auf "OK".

Erstellen und Konfigurieren von Organisationsgruppen

Jede Organisationsübersicht enthält eine oder mehrere Organisationsgruppen, die jeweils wiederum Ressourcen und untergeordnete Organisationsgruppen enthalten können. Die Hierarchiestruktur der Organisationsgruppen kann beliebig viele Ebenen haben, um die Ressourcen in Ihrer Umgebung darzustellen. Die Mitgliedschaft in einer Organisationsgruppe umfasst die Ressourcen, die in allen untergeordneten Gruppen enthalten sind.

Die Symantec Management Console enthält eine Standard -Organisationsansicht, in der alle Ressourcen automatisch abgelegt werden. Die Standardstruktur ist eine Hierarchie von Organisationsgruppen, basierend auf dem Ressourcentyp. Sie können keine Organisationsgruppen der Standard -Organisationsansicht hinzufügen und keine daraus entfernen. Alle neu erkannten Ressourcen werden automatisch in der entsprechenden Gruppe in der Standard -Organisationsansicht abgelegt.

Diese Aufgabe ist ein Schritt beim Konfigurieren der Ressourcensicherheit.

Siehe "Konfigurieren der Ressourcensicherheit" auf Seite 355.

So erstellen und konfigurieren Sie eine Organisationsgruppe

1. Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Organisationsansichten und Gruppen".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf die Organisationsansicht, der eine neue Organisationsgruppe hinzugefügt werden soll, und klicken Sie dann auf "Neu > Organisationsgruppe".
3. Bearbeiten Sie im rechten Teilfenster den Namen und die Beschreibung der Organisationsgruppe.

   Gruppennamen unterliegen keinerlei Beschränkungen. Daher sind mehrere Gruppen mit dem gleichen Namen möglich.
4. So fügen Ressourcen der Gruppe hinzu

   - Klicken Sie im rechten Teilfenster auf "Hinzufügen" und dann auf das Element, das Sie der Gruppe hinzufügen möchten.

- Wählen Sie im Dialogfeld "Gruppe bearbeiten" die entsprechenden Ressourcen aus und klicken Sie dann auf "OK".

5 Klicken Si zum Entfernen einer Ressource aus der Gruppe mit der rechten Maustaste auf die Ressource und wählen Sie im Kontextmenü die Option "Löschen".

Warnung: Wenn Sie eine Ressource löschen, wird sie aus CMDB entfernt. Sie sollten keine Ressourcen löschen, die für Symantec Management-Plattformaktivitäten und -funktionalität wichtig sind. Zu den kritische Ressourcen gehören der Notification Server-Computer, -Sites und -Subnetze.

Anzeigen von Ressourcen in einer Organisationsgruppe

Die Fenster "Ressourcen" zeigt alle Ressourcen an, die direkt in der Organisationsgruppe enthalten sind, sowie alle Ressourcen, die in untergeordneten Gruppen enthalten sind. Sie können die Ansicht so ändern, dass nur die Computer in der Gruppe angezeigt werden.

Siehe "Konfigurieren der Ressourcensicherheit" auf Seite 355.

Sie können die Liste der Ressourcen anzeigen, die für eine bestimmte Sicherheitsrolle verfügbar sind. Beispielsweise empfiehlt es sich zu überprüfen, ob Sie die Ressourcensicherheit für eine bestimmte Rolle korrekt eingerichtet haben. Die einer Organisationsgruppe zugewiesenen Sicherheitsrollen legen den Zugriff auf alle Ressourcen fest, die direkt in dieser Gruppe enthalten sind. Jede Sicherheitsrolle hat nur auf diejenigen Ressourcen Zugriff, die direkt in den Gruppen enthalten sind, denen die Rolle zugewiesen wird.

Wenn Sie die Ressourcen für eine bestimmte Sicherheitsrolle anzeigen, sehen Sie nur diejenigen Ressourcen, die für die ausgewählte und Ihre Rolle verfügbar sind. Wenn es sich bei Ihrer Rolle um die Rolle "Administrator" handelt (die Zugriff auf alle Ressourcen hat), sehen Sie immer alle Ressourcen, die für die ausgewählte Rolle verfügbar sind. Wenn Sie jedoch eine andere Rolle haben (die möglicherweise keinen Zugriff auf alle Ressourcen hat), können Sie möglicherweise nicht alle Ressourcen sehen, die für die ausgewählte Rolle verfügbar sind.

Hinweis: Wenn Sie nicht zu einer Rolle gehören (d. h. benutzerbasierte statt rollenbasierte Sicherheit wurde angewendet), wählen Sie "Kein(e)", damit keine Sicherheitsrolle ausgewählt ist. Dadurch wird sichergestellt, dass alle Ressourcen gezeigt werden, auf die Sie Zugriff haben. Wenn Sie eine Rolle auswählen, zu der Sie nicht gehören, werden alle Ressourcen herausgefiltert und nichts wird angezeigt.

Sie können Verwaltungsaktionen für Ressourcen in einer Organisationsgruppe durchführen. Zu den verfügbaren Aktionen gehören das Öffnen des Ressourcenmanagers, das Exportieren der Ressource in eine XML-Datei, das Anzeigen der Ressourceneigenschaften, das Hinzufügen der Ressource zu einer anderen Gruppe und das Löschen der Ressource aus der Gruppe.

So zeigen Sie Ressourcen in einer Organisationsgruppe an

1. Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Organisationsansichten und Gruppen".
2. Erweitern Sie im linken Teilfenster den Ordner "Organisationsansichten" und wählen Sie anschließend die gewünschte Organisationsgruppe aus.
3. (Optional) Klicken Sie zum Anzeigen von Ressourcen für eine bestimmte Sicherheitsrolle im rechten Teilfenster unter "Ressourcen" in der Dropdown-Liste "Rolle" auf die gewünschte Rolle.

Festlegen der Sicherheit für eine Organisationsgruppe

Die Sicherheit für eine Organisationsgruppe wird durch Zuweisen der entsprechenden Sicherheitsrollen festgelegt. Wenn eine Sicherheitsrolle einer Gruppe zugewiesen wird, haben die Mitglieder dieser Sicherheitsrolle Zugriff auf die in der Gruppe enthaltenen Ressourcen. Standardmäßig erben alle untergeordneten Gruppen alle Sicherheitszuweisungen der Organisationsgruppe. Die Vererbung gibt der Rolle den gleichen Zugriff auf alle Ressourcen in den untergeordneten Gruppen. Sie können die Vererbung auf einer beliebigen Ebene unterbrechen und bei Bedarf wiederherstellen.

Zum Einstellen der Sicherheit für Organisationsgruppen benötigen Sie die Berechtigung zum Ändern von Berechtigungen.

Bei der Installation der Symantec Management-Plattform gibt die Standardkonfiguration allen Rollen die volle Berechtigung für die Standard -Organisationsansicht. Die Standardkonfiguration gibt allen Rollen den vollen Zugriff auf alle Ressourcen. Bei der (optionalen) Konfiguration der Ressourcensicherheit können Sie die Standard -Organisationsansicht zum Zuweisen der Standardberechtigungen für alle Ressourcen oder bestimmte Ressourcentypen benutzen. Sie müssen die Vererbung für die entsprechenden Sicherheitsrollen deaktivieren und die Berechtigungen weiter unten in der Organisationsgruppenstruktur löschen.

Sie können einer Organisationsgruppe eine Sicherheitsrolle mit den für diese Rolle erforderlichen Berechtigungen zuweisen. So erfordert zum Beispiel eine Admistratorrolle die vollständigen Verwaltungsrechte für alle Ressourcen in einer Gruppe. Die Endbenutzerrolle dagegegen erfordert vielleicht nur den Lesezugriff auf diese Ressourcen. Standardmäßig gehen die Berechtigungen einer

Sicherheitsrolle für eine Organisationsgruppe auch auf alle ihre untergeordneten Gruppen über.

Diese Aufgabe ist ein Schritt beim Konfigurieren der Ressourcensicherheit.

Siehe "Konfigurieren der Ressourcensicherheit" auf Seite 355.

So legen Sie die Sicherheit für eine Organisationsgruppe fest

1. Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Organisationsansichten und Gruppen".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf die Organisationsgruppe, wählen Sie im Kontextmenü die Option "Sicherheit verwalten" und dann eine der folgenden:

So weisen Sie alle verfügbaren Berechtigungen zu	■ Klicken Sie auf "Verwaltungsrechte zuweisen". ■ Wählen Sie im Dialogfeld "Verwaltungsrechte zuweisen" die gewünschten Sicherheitsrollen aus und klicken Sie dann auf "OK".
So weisen Sie die Symantec-Leserechte zu	■ Klicken Sie auf "Leserechte zuweisen...". ■ Wählen Sie im Dialogfeld "Leserechte zuweisen" die gewünschten Sicherheitsrollen aus und klicken Sie dann auf "OK".
So legen Sie benutzerdefinierte Sicherheitsberechtigungen fest	■ Klicken Sie auf "Benutzerdefinierte Rechte zuweisen". ■ Wählen Sie im Sicherheitsrollenmanager in der Dropdown-Liste "Rolle" die Sicherheitsrolle aus, für die Sie benutzerdefinierte Berechtigungen festlegen möchten. ■ Klicken Sie in der Dropdown-Liste "Ansicht" auf "Alle Elemente". ■ Wählen Sie im linken Teilfenster die Organisationsansicht bzw. -gruppe aus, für die Sie Berechtigungen festlegen möchten. ■ Nehmen Sie im rechten Teilfenster unter "Nicht geerbt" die entsprechenden Änderungen an den Berechtigungseinstellungen vor. ■ (Optional) Wenn Sie die Berechtigungsvererbung konfigurieren möchten, klicken Sie auf "Erweitert". Siehe "Anpassen der Vererbungsregeln für Berechtigungen" auf Seite 109. ■ Klicken Sie auf "Änderungen speichern".

3. Klicken Sie auf "Änderungen speichern".

Überlegungen zu Ressourcen mit Bereichsfestlegung

Ressourcen mit Bereichsfestlegung stellt eine sichere Methode bereit, Ressourcen in leicht verwaltbare, gut strukturierte Einheiten zu teilen. Da diese Einheiten allgemein sind, können sie so angeordnet werden, dass sie eine Vielzahl unterschiedlicher organisatorischer Anforderungen erfüllen können.

In den meisten Fällen müssen zum Einschätzen der Anforderungen für die Ressourcen mit Bereichsfestlegung innerhalb Ihrer Umgebung folgende Fragen beantwortet werden:

- Wer soll vollen Zugriff auf die Infrastruktur der Symantec Management-Plattform haben?
- Welche Rollen sind innerhalb der Verwaltungsfunktionen für alltägliche Vorgänge vorhanden?
- Welche Funktionsbereiche erfordern besondere Rollen und Rechte?
- Spiegelt Active Directory unser Verwaltungs- und Geschäftsmodell wider?
- Existieren Active Directory-Gruppen, die den Rollen innerhalb der Architektur der Symantec Management-Plattform entsprechen?
- Welche Arten von Ressourcen müssen verwaltet werden?

Verwenden Sie bei der Entwicklung eines Ressourcen-Frameworks die folgende Implementierungsprüfliste, um sicherzustellen, dass die Entwicklung in der richtigen Reihenfolge abgeschlossen wird:

- Identifizieren Sie Benutzer, Sicherheitsrollen und Rechte.
- Erstellen Sie Sicherheitsrollen.
  Weisen Sie Rechte und Benutzermitgliedschaft zu.
- Erstellen Sie Organisationsansichten und Gruppenstrukturen.
  Halten Sie die bewährten Verfahren für den AD-Import ein. Gruppieren Sie nach Ressourcentyp (Benutzer, Computer).
- Rollen und Berechtigungen bestimmten Organisationsansichten und Gruppen zuweisen.
- Berichte für die Basissystemansicht von Ressourcen generieren.
- Sichern Sie die Organisationsansicht und Gruppenstruktur mithilfe von XML-Export.

Tabelle 22-2 Stellen Sie Überlegungen zu Ressourcen mit Bereichsfestlegung an.

Element	Überlegungen anstellen
Sicherheit	■ Sie sollten Sicherheitsrollen einrichten, bevor Sie andere Konsolensicherheitsaufgaben ausführen und bevor Notification Server in Ihrer Produktionsumgebung bereitgestellt wird. ■ Ressourcensicherheit ist die Kombination von Bereich, Sicherheitsrolle und Berechtigungen. ■ Ressourcen beziehen alle ihre Berechtigungsbewilligungen von den Bereichsammlungen, deren Mitglied sie sind. Die Bewilligungen sind kumulativ. Durch eine Berechtigung zum Ausführen einer Aktion auf einer Ressource in einer Bereichssammlung stellen Sie sicher, dass der Benutzer bzw. die Rolle diese Aktion auch dann durchführen kann, wenn die Berechtigung auf andere Bereichssammlungen angewendet wird, die die Ressource enthalten. ■ Sicherheitsrollen sind Benutzergruppen, denen Sie Rechte für Administrator-/Arbeitsaufgaben und Berechtigungen für Ordner oder Elemente zuweisen können, die diese Administratoren/Arbeitskräfte in der Symantec Management Console anzeigen können. ■ Die standardmäßigen Rollen verfügen über eine Reihe von Berechtigungsbewilligungen. Rollen können außerdem an einer beliebigen Stelle in der Organisationsansicht oder Organisationsgruppenstruktur zugewiesen werden, je nach dem zu gewährenden Verwaltungsumfang. ■ Sicherheitsbewilligungen werden Organisationsgruppen zugewiesen und von der darüberliegenden Organisationsgruppe geerbt.

Element	Überlegungen anstellen
Organisationsansichten	

Element	Überlegungen anstellen
	■ Eine Organisationsansicht ist eine selbstständige Hierarchie von Organisationsgruppen, die Ressourcen enthalten. ■ Organisationsansichten stellen eine vereinfachte und sichere Methode zum Gruppieren und Verwalten von Ressourcen dar. ■ Verwenden Sie gegebenenfalls eine Organisationsansicht, um eine Ihrer IT-Umgebung entsprechende administrative Sicherheitsstruktur oder Grenze darzustellen. ■ Spiegeln Sie das Organisationsmodell Ihres Active Directory mithilfe der Funktion "Active Directory-Import", um das manuelle Erstellen und Auffüllen zu vermeiden. ■ Für alle Ressourcen in einer Organisationsansicht (verwaltete und nicht verwaltete) wird standardmäßig eine Bereichsfestlegung durchgeführt. ■ Organisationsansichten enthalten Organisationsgruppen, die wiederum Ressourcen enthalten. Organisationsansichten können Ressourcen nicht direkt enthalten. Alle neu erkannten Ressourcen werden automatisch in die standardmäßige Organisationsansicht importiert. ■ Ein Ressourcenelement kann in jeder Organisationsansicht nur zu einer Organisationsgruppe gehören. Wenn Sie einer Organisationsgruppe eine Ressource hinzufügen, wird sie automatisch aus einer anderen Gruppe, der sie möglicherweise zugewiesen ist, entfernt. ■ Verwenden Sie Organisationsgruppen, um eine Richtlinie oder Aufgabe auf ausgewählte Computer, Benutzer und Ressourcen anzuwenden. Verwenden Sie hierzu eine Organisationsgruppe in einem Ziel. In dieser Instanz dient die Organisationsgruppe als Filter. Durch Sicherheitsfunktionen wird sichergestellt, dass nur die Ressource aufgenommen wird, für die der Besitzer des Ziels Berechtigungen besitzt. ■ In der Symantec Management-Plattform sind mehrere Organisationsansichten möglich, weil Administratoren die Ressourcen eventuell unterschiedlich organisieren. Deshalb verfügen Sie über eine nach Funktion und eine nach Region geordnete Ansicht. ■ Bei der standardmäßigen Organisationsansicht werden alle Ressourcen Bereichen zugeordnet und sind sicher. Die Ressourcen (verwaltete und nicht verwaltete) werden nach Typ gruppiert und die Ressourcenmitgliedschaft ist dynamisch. ■ Die Ressourcenmitgliedschaft in der Systemstandardansicht wird dynamisch aktualisiert. Das Aktualisierungsintervall beträgt 5 Minuten. Abhängig davon, wie Sie die Erstellung und Ressourcenmitgliedschaft Ihrer Organisationsstruktur planen,

Element	Überlegungen anstellen
	müssen Sie dies berücksichtigen, wenn Sie die allgemeinen Auswirkungen der Aktualisierung der Ressourcenmitgliedschaft identifizieren.
Filter	■ Filter sind ähnlich aufgebaut wie Sammlungen von Notification Server 6. Jedoch unterscheiden sie sich in der Implementierung, da sie auf Ziele und nicht auf Richtlinien angewendet werden. Es handelt sich um Ressourcen, die durch einen definierten Satz von Kriterien verbunden sind. ■ Filter sollten von einem einzelnen Attribut erstellt werden. Durch die Kombination von Filtern können Sie komplexe Ziele erstellen und durch die Verwendung weniger Kriterien kann die Wahrscheinlichkeit der Wiederverwendung erhöht und die Komplexität verringert werden. Dadurch erhalten Sie einen leistungsfähigeren Notification Server.
Ziele	■ Ziele stellen den Schnittpunkt von Organisationsgruppen und Filtern dar. Beispielsweise alle Computer in der Finanzierung (Gruppe), die über weniger als 1 GB RAM (Filter) verfügen. ■ Ziele werden auf Richtlinien und Aufgaben angewendet und können vorab oder zum Zeitpunkt ihrer Anwendung erstellt werden. ■ Ziele können nur die Ressourcen enthalten, auf die der Ersteller des Ziels Zugriff hat. Zwar sind sie als Objekte in der Konsole nicht sichtbar, durch die Option "Schnellzuordnung" in einer Aufgabe oder Richtlinie kann jedoch auf sie zugegriffen werden.

Kapitel 23

Konfigurieren der Ressourcenfilter und -ziele

In diesem Kapitel werden folgende Themen behandelt:

- Info zu Ressourcenfiltern
- Erstellen oder Ändern von Filtern
- Durchführen von Aktionen für Filterressourcen
- Anzeigen von Filterabhängigkeiten
- Info zu Ressourcenzielen
- Planen von Ressourcen-Mitgliedschaftsaktualisierungen

Info zu Ressourcenfiltern

Ein Filter, auch Ressourcenfilter genannt, ist eine dynamische Definition eines Ressourcensatzes. Die Ressourcen können nach angegebenen Parametern gruppiert werden und können auch explizit in einem Filter enthalten oder davon ausgeschlossen sein. Ein Filter isoliert gewöhnlich nur einen Aspekt einer Ressource, wie zum Beispiel sein Betriebssystem, den verfügbaren Festplatten- oder RAM-Speicher. Filter werden mit Organisationsgruppen zur Identifizierung der Ressourcen (Ressourcenziel) verwendet, auf die eine Aufgabe oder Richtlinie angewendet wird.

Siehe "Info zu Ressourcenzielen" auf Seite 383.

Ein Filter enthält keine bestimmten Ressourcen. Alle Ressourcen sind in den Organisationsgruppen enthalten, die in Organisationsansichten eingerichtet werden. Die Organisationsgruppen und Organisationsansichten sind dieselben, die auch für die Ressourcensicherheit verwendet werden. Ein Filter wird auf eine bestimmte

Organisationsansicht oder -gruppe angewendet, um die entsprechenden Ressourcen zu identifizieren. Folglich sind Filter portabel, können auf jede Organisationsansicht oder -gruppe angewendet und mit anderen Filtern verwendet werden. Beispielsweise empfiehlt es sich, eine Richtlinie auf alle Windows XP-Computer in einer bestimmten Abteilung Ihrer Organisation anzuwenden. Wenn Sie in diesem Fall nur die Computer mit Windows XP auswählen möchten, können Sie einen Filter auf die Organisationsgruppe anwenden, die für die entsprechende Abteilung steht.

Siehe "Erstellen oder Ändern von Filtern" auf Seite 370.

Erstellen oder Ändern von Filtern

Sie können Filter komplett neu erstellen oder einen vorhandenen Filter duplizieren und dann entsprechend ändern. Sämtliche von Ihnen erstellte Filter oder solche, für die Sie eine Schreibberechtigung haben, können von Ihnen geändert werden. Sie können die Standardfilter, die mit Notification Server ausgeliefert werden, nicht ändern. Sie können keine Filter ändern, die durch Hierarchiereplikation von einem übergeordneten Notification Server hinzugefügt wurden. Nur die Filter, die auf Ihrem Notification Server erstellt wurden, können lokal bearbeitet werden.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Sie können einen Filter auch durch Speichern eines Berichts erstellen. Ein so erstellter Filter ist statisch und enthält keine Abfrage. Die Filtermitgliedschaft ist eine festgelegte Liste von Einschlüssen. Sie wird während der Filtererstellung bestimmt. Sie können einen statischen Filter ändern, indem Sie weitere Einbeziehungen oder Ausnahmen hinzufügen, die dynamische Filter sein können. Jedoch können Sie eine Abfrage nicht direkt einem statischen Filter hinzufügen.

Siehe "Erstellen eines statischen Filters aus Notification Server-Berichtergebnissen" auf Seite 467.

Tabelle 23-1 Verfahren zum Erstellen oder Ändern von Filtern

Schritt	Aktion	Beschreibung
Schritt 1	Erstellen Sie einen neuen Filter oder wählen Sie einen vorhandenen Filter zum Bearbeiten aus.	Sie können einen ganz neuen Filter erstellen oder einen vorhandenen Filter Ihren Anforderungen entsprechend ändern. Siehe "Erstellen eines neuen Filters" auf Seite 372. Siehe "Ändern eines vorhandenen Filters" auf Seite 372.

Schritt	Aktion	Beschreibung
Schritt 2	Wählen Sie den Abfragetyp aus.	Dieser Schritt bezieht sich nur auf neue Filter. Beim Ändern eines vorhandenen Filters kann der Abfragetyp nicht geändert werden. Wenn Sie einen dynamischen Filter erstellen möchten, müssen Sie den entsprechenden Abfragetyp auswählen. Wird keine Abfrage ausgewählt, entspricht die Filtermitgliedschaft den angegebenen Ein- und Ausschlüssen. Siehe "Auswählen des Filterabfragetyps" auf Seite 373.
Schritt 3	Legen Sie die zu verwendende Abfrage fest.	Sie können den Abfrage-SQL-Code entweder selbst schreiben oder die Abfrage mit dem Abfragegenerator erstellen. Der Abfragegenerator ist ein benutzerfreundliches Tool, mit dem Sie die gewünschten Tabellen und Felder auswählen können. Mit ihm können Sie die Abfrage Ihren Anforderungen entsprechend definieren. Siehe "Definieren einer Ressourcenabfrage für einen Filter" auf Seite 374. Siehe "Definieren einer SQL-Abfrage für einen Filter" auf Seite 377.
Schritt 4	Geben Sie die Ein- und Ausschlüsse an.	Sie können bestimmte Ressourcen oder Filter angeben, die im Filter ein- oder ausgeschlossen werden sollen. Die ein- oder auszuschließenden Filter können weitere Filter enthalten. Sie können aus den in der CMDB gespeicherten Ressourcen und Filtern auswählen oder Ressourcen aus einer CSV-Datei importieren. Siehe "Ein- und Ausschließen von Elementen in/aus Filtern" auf Seite 378.
Schritt 5	Überprüfen Sie die Filterkonfiguration durch Anzeigen der Filtermitgliedschaft.	Die Mitgliedschaft eines Filters wird festgelegt, indem die Filterabfrage in der CMDB ausgeführt wird, um die entsprechenden Ressourcen zu extrahieren. Sie können die Mitgliedschaft aktualisieren, um zu überprüfen, ob der Filter richtig definiert wurde. Siehe "Aktualisieren der Mitgliedschaft eines Filters" auf Seite 380.
Schritt 6	Speichern Sie den Filter.	Sie können die neue oder geänderte Filterdefinition speichern. Sobald ein neuer Filter gespeichert wurde, kann der zugehörige Abfragetyp nicht mehr geändert werden. Siehe "Erstellen eines neuen Filters" auf Seite 372. Siehe "Ändern eines vorhandenen Filters" auf Seite 372.

Erstellen eines neuen Filters

Sie können neue Filter erstellen und die Abfrage, Einschlüsse und Ausnahmen angeben, um die gewünschte Mitgliedschaft zu definieren.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Diese Aufgabe ist ein Schritt beim Erstellen bzw. Ändern von Filtern.

Siehe "Erstellen oder Ändern von Filtern" auf Seite 370.

So erstellen Sie einen neuen Filter

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Filter".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, in dem Sie den neuen Filter hinzufügen möchten, und klicken Sie dann auf "Neu > Filter".
3. Geben Sie im rechten Teilfenster den Filternamen und die Beschreibung an.
4. Wählen Sie den Abfragetyp aus.

   Siehe "Auswählen des Filterabfragetyps" auf Seite 373.
5. Führen Sie einen der folgenden Schritte aus:

Definieren Sie die Abfrage	Siehe "Definieren einer Ressourcenabfrage für einen Filter" auf Seite 374. Siehe "Definieren einer SQL-Abfrage für einen Filter" auf Seite 377.
Geben Sie alle notwendigen Einschlüsse und Ausnahmen an	Siehe "Ein- und Ausschließen von Elementen in/aus Filtern" auf Seite 378.
Aktualisieren Sie die Filtermitgliedschaft	Siehe "Aktualisieren der Mitgliedschaft eines Filters" auf Seite 380.

6. Klicken Sie auf "Änderungen speichern".

Ändern eines vorhandenen Filters

Sämtliche von Ihnen erstellte Filter oder solche, für die Sie eine Schreibberechtigung haben, können von Ihnen geändert werden. Sie können die Standardfilter, die mit Notification Server ausgeliefert werden, nicht ändern. Sie können keine Filter ändern, die durch Hierarchiereplikation von einem übergeordneten Notification Server hinzugefügt wurden. Nur die Filter, die auf Ihrem Notification Server erstellt wurden, können lokal bearbeitet werden. Die einzige Aktion, die Sie für einen

schreibgeschützten Filter durchführen können, ist das Aktualisieren der Filtermitgliedschaft.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Wenn Sie einen schreibgeschützten Filter ändern möchten, duplizieren Sie ihn, um einen neuen Filter zu erstellen und ihn dann Ihren Anforderungen entsprechend zu ändern. Wenn Sie einen Filter ändern, können Sie die Filterabfrage und die spezifischen Ein- oder Ausschlüsse ändern, jedoch nicht den Abfragetyp.

Diese Aufgabe ist ein Schritt beim Erstellen bzw. Ändern von Filtern.

Siehe "Erstellen oder Ändern von Filtern" auf Seite 370.

So ändern Sie einen vorhandenen Filter

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Filter".
2. Klicken Sie im linken Teilfenster auf den Filter, den Sie bearbeiten möchten.
3. (Optional) Ändern Sie im rechten Teilfenster den Filternamen und die Beschreibung.
4. Klicken Sie oben rechts auf "Bearbeiten".

   Wenn die Option "Bearbeiten" nicht verfügbar ist, ist der Filter schreibgeschützt und kann nicht geändert werden.
5. Führen Sie eine der folgenden Aktionen aus:

Abfrage ändern	Siehe "Definieren einer Ressourcenabfrage für einen Filter" auf Seite 374. Siehe "Definieren einer SQL-Abfrage für einen Filter" auf Seite 377.
Ein- und Ausschlüsse ändern	Siehe "Ein- und Ausschließen von Elementen in/aus Filtern" auf Seite 378.
Filtermitgliedschaft aktualisieren	Siehe "Aktualisieren der Mitgliedschaft eines Filters" auf Seite 380.

6. Klicken Sie auf "Änderungen speichern".

Auswählen des Filterabfragetyps

Wenn Sie einen neuen Filter erstellen, muss der Typ der zu verwendenden Abfrage angegeben werden. Entweder Sie erstellen die Filterabfrage mit dem Abfragegenerator oder Sie schreiben die SQL-Abfrage selbst. Der Filter muss dabei

keine Abfrage enthalten. Nachdem der Filter gespeichert wurde, kann der Abfragetyp nicht mehr geändert werden.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Diese Aufgabe ist ein Schritt beim Erstellen bzw. Ändern von Filtern.

Siehe "Erstellen oder Ändern von Filtern" auf Seite 370.

So wählen Sie den Filterabfragetyp aus

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Filter".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, in dem Sie den neuen Filter hinzufügen möchten, und klicken Sie dann auf "Neu > Filter".
3. Wählen Sie auf der Seite "Neuer Filter" in der Dropdown-Liste "Filterdefinition" den Abfragetyp aus, den Sie verwenden möchten:

Keiner	Der Filter verwendet keine Abfrage. Die Ein- und Ausschlüsse bestimmter Ressourcen und Filter bestimmen die Filtermitgliedschaft.
Abfragegenerator	Verwenden Sie den Abfragegenerator, um die Filterabfrage zu erstellen. Der Abfragegenerator ist ein benutzerfreundliches Tool, mit dem Sie die gewünschten Tabellen und Felder auswählen können. Mit ihm können Sie die Abfrage Ihren Anforderungen entsprechend definieren. Siehe "Definieren einer Ressourcenabfrage für einen Filter" auf Seite 374.
Rohes SQL	Schreiben Sie Ihre eigene SQL-Abfrage. Beispielsweise möchten Sie eine Abfrage aus einem anderen Filter oder Bericht kopieren und entsprechend Ihren Anforderungen ändern. Siehe "Definieren einer SQL-Abfrage für einen Filter" auf Seite 377.

Definieren einer Ressourcenabfrage für einen Filter

Eine Ressourcenabfrage beruht auf den in der CMDB verfügbaren Tabellen. Der Abfragegenerator ist ein benutzerfreundliches Tool, das eine Standardvorlage zur Verfügung stellt und die Auswahl gewünschter Tabellen und Felder erlaubt. Mit ihm können Sie die Abfrage wunschgemäß definieren. Dabei sind keine SQL-Kenntnisse erforderlich. Die Ressourcenabfrage wird automatisch in SQL konvertiert. Dieser Code wird dann in der CMDB ausgeführt, um die entsprechenden Ressourcen zu extrahieren.

Siehe "Auswählen des Filterabfragetyps" auf Seite 373.

Diese Aufgabe ist ein Schritt beim Erstellen bzw. Ändern von Filtern.

Siehe "Erstellen oder Ändern von Filtern" auf Seite 370.

So definieren Sie eine Ressourcenabfrage für einen Filter

1. Klicken Sie in Symantec Management Console im Menü "Verwalten" auf "Filter".
2. Klicken Sie im linken Bereich auf den Filter, den Sie bearbeiten möchten.
3. Geben Sie im rechten Teilfenster im Bereich "Filterdefinition" die Ressourcenabfragedetails auf den entsprechenden Registerkarten an.

Abfrage	Die Syntax der Ressourcenabfrage. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrage" " auf Seite 553.
Felder	Die in der Abfrage zu verwendenden Felder und Datenklassenattribute. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Felder" " auf Seite 557.
Abfrageparameter	Die Parameter, die in der Abfrage verwendet werden. Dies sind interne Parameter für SQL-Verwendung, keine Benutzerparameter. Parameter werden gewöhnlich nicht in Filterabfragen verwendet, können aber beim Abruf von Registrierungsinformationen hilfreich sein. Dabei kann es sich um eine Agent-Versionsnummer für ein Upgrade handeln. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageparameter" " auf Seite 559.
Filterausdrücke	Die Bedingungsanweisungen, die verwendet werden, um die Ergebnisse der Abfrage weiter zu verfeinern. Jede Anweisung oder gruppierte Anweisung kann als Filter betrachtet werden. Sie müssen die Anweisungen erstellen, die Sie verwenden möchten, und sie entsprechend gruppieren. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Filterausdrücke" " auf Seite 560.
Abfrageauflösung	Der SQL-Code, der zur Extraktion der Filterergebnisse für die CMDB ausgeführt wird. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageauflösung" " auf Seite 563.

Definieren einer SQL-Abfrage für einen Filter

Sie können eine SQL-Abfrage schreiben, um die Ressourcen zu definieren, die im Filter enthalten sein sollen. Sie können den SQL-Code von Grund auf schreiben. Alternativ können Sie SQL aus einem anderen Filter oder Bericht kopieren und Ihren Anforderungen entsprechend ändern. Beispielsweise können Sie eine Ressourcenabfrage mit dem Abfragegenerator erstellen und anschließend das generierte SQL aus der Registerkarte "Abfrageauflösung" kopieren. Sie können den Abfragegenerator auch verwenden, um die grundlegende Struktur der Abfrage festzulegen, diese in SQL-Code zu konvertieren und den Code dann direkt anzupassen, um die gewünschte Abfrage zu erstellen.

Sie benötigen die Berechtigung zum Bearbeiten von SQL, um SQL-Abfragen zu erstellen oder zu ändern. Zudem sollten Sie sich mit der CMDB-Tabellenstruktur auskennen.

Siehe "Auswählen des Filterabfragetyps" auf Seite 373.

Diese Aufgabe ist ein Schritt beim Erstellen bzw. Ändern von Filtern.

Siehe "Erstellen oder Ändern von Filtern" auf Seite 370.

So definieren Sie eine SQL-Abfrage für einen Filter

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Filter".
2. Klicken Sie im linken Teilfenster auf den Filter, den Sie bearbeiten möchten.

3 Geben Sie im rechten Teilfenster im Bereich "Filterdefinition" die SQL-Abfragedetails auf den entsprechenden Registerkarten an.

Parameterisierte Abfrage	Der SQL-Code für die Abfrage. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Parametrisierte Abfrage" " auf Seite 558.
Abfrageparameter	Die Parameter, die in der Abfrage verwendet werden. Dies sind interne Parameter für SQL-Verwendung, keine Benutzerparameter. Parameter werden gewöhnlich nicht in Filterabfragen verwendet, können aber beim Abruf von Registrierungsinformationen hilfreich sein. Dabei kann es sich um eine Agent-Versionsnummer für ein Upgrade handeln. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageparameter" " auf Seite 559.
Abfrageauflösung	Der SQL-Code, der zur Extraktion der Filterergebnisse für die CMDB ausgeführt wird. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageauflösung" " auf Seite 563.

4 Klicken Sie auf "Änderungen speichern".

Ein- und Ausschließen von Elementen in/aus Filtern

Sie können bestimmte Ressourcen oder Filter angeben, die im Filter ein- oder ausgeschlossen werden sollen. Die ein- oder auszuschließenden Filter können weitere Filter enthalten. Sie können Ressourcen und Filter aus der Liste der verfügbaren Elemente in CMDB auswählen oder Sie können Ressourcen aus einer CSV-Datei importieren.

Wenn Sie , identifizieren möglicherweise Ressourcen aus einer CSV-Datei importieren, kann die Datei einen Computer über seinen Namen, seinen vollständig qualifizierten Domänennamen oder seine IP-Adresse identifizieren. Alle Elemente, die nicht in CMDB gefunden werden, werden ignoriert.

Die Filtermitgliedschaft wird festgelegt, indem man die Einschlüsse den Abfrageergebnissen hinzufügt, und dann die Ausnahmen entfernt. Filter und Ressourcen haben keinen Unterschied in der Priorität.

Diese Aufgabe ist ein Schritt beim Erstellen bzw. Ändern von Filtern.

Siehe "Erstellen oder Ändern von Filtern" auf Seite 370.

So geben Sie an, welche Ressourcen ein- oder ausgeschlossen werden sollen

1. Klicken Sie in Symantec Management Console im Menü "Verwalten" auf "Filter".
2. Klicken Sie im linken Teilfenster auf den Filter, den Sie bearbeiten möchten.
3. Im rechten Teilfenster im Bereich "Filterdefinition" unter "Explizite Ein- und Ausschlüsse" haben Sie folgende Optionen:

So schließen Sie ausgewählte Ressourcen ein	1 Unter "Einschlüsse" klicken Sie auf "Ressource auswählen". 2 Im Fenster "Ressourcen auswählen" wählen Sie die Ressourcen aus, die Sie einschließen möchten, und klicken dann auf "OK".
So schließen die Ressourcen ein, die in einer Datei aufgelistet werden	1 Unter "Einschlüsse" klicken Sie auf "Aus Datei importieren". 2 Wählen Sie im Fenster "Zu importierende Datei auswählen" die entsprechende CSV-Datei aus und klicken Sie anschließend auf "Öffnen".
So schließen Sie ausgewählte Ressourcen aus	1 Unter "Ausschlüsse" klicken Sie auf "Ressource auswählen". 2 Im Fenster "Ressourcen auswählen" wählen Sie die Ressourcen aus, die Sie ausschließen möchten, und klicken dann auf "OK".
So schließen die Ressourcen aus, die in einer Datei aufgelistet werden	1 Unter "Ausschlüsse" klicken Sie auf "Aus Datei importieren". 2 Wählen Sie im Fenster "Zu importierende Datei auswählen" die entsprechende CSV-Datei aus und klicken Sie anschließend auf "Öffnen".

Die ausgewählten Ressourcen werden neben den entsprechenden Feldern aufgelistet.

So geben Sie an, welche Filter ein- oder ausgeschlossen werden sollen

1. Klicken Sie in Symantec Management Console im Menü "Verwalten" auf "Filter".
2. Klicken Sie im linken Teilfenster auf den Filter, den Sie bearbeiten möchten.
3. Im rechten Teilfenster im Bereich "Filterdefinition" unter "Explizite Ein- und Ausschlüsse" haben Sie folgende Optionen:

So schließen Sie ausgewählte Filter ein	1 Unter "Einschlüsse" klicken Sie auf "Filter auswählen". 2 Im Fenster "Filter auswählen" wählen Sie die Filter aus, die Sie einschließen möchten, und klicken dann auf "OK".
So schließen Sie ausgewählte Filter aus	1 Unter "Ausschlüsse" klicken Sie auf "Filter auswählen". 2 Im Fenster "Filter auswählen" wählen Sie die Filter aus, die Sie ausschließen möchten, und klicken dann auf "OK".

Die ausgewählten Filter werden neben den entsprechenden Feldern aufgelistet.

Aktualisieren der Mitgliedschaft eines Filters

Die Mitgliedschaft eines Filters wird festgelegt, indem die Filterabfrage in der CMDB ausgeführt wird, um die entsprechenden Ressourcen zu extrahieren. Um die Filtermitgliedschaft auf dem aktuellen Stand zu halten, wenn sich die Ressourceninformationen in der CMDB ändern, sollten Sie die Mitgliedschaft in geeigneten Intervallen aktualisieren. Sie können die geplanten Filteraktualisierungen verwenden, um die Filtermitgliedschaft zu aktualisieren, oder Sie können die Aktualisierung zu den entsprechenden Zeitpunkten manuell ausführen. Wenn Sie beispielsweise einen Filter erstellen oder ändern, können Sie die Mitgliedschaft aktualisieren, um zu überprüfen, ob der Filter richtig definiert ist.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Siehe "Planen von Ressourcen-Mitgliedschaftsaktualisierungen" auf Seite 384.

Der Bereich "Filtermitgliedschaft" auf der Seite *"Filtername"* zeigt die Details der Ressourcen in Ihrem Bereich an, die derzeit als Mitglieder des Filters identifiziert sind. Die Filtermitgliedschaft ist möglicherweise für verschiedene Benutzerrollen unterschiedlich. Die Ressourcen sind nur für die Benutzer mit "Leseberechtigung" sichtbar. Wenn Jedoch ein Benutzer die Mitgliedschaft eines Filters manuell aktualisiert, wird die Filterabfrage für alle Ressourcen in der CMDB ausgeführt. Die Konsole schränkt die Ergebnisse ein, damit nur die Ressourcen angezeigt werden, die innerhalb des Anzeigebereichs des Benutzers liegen.

Diese Aufgabe ist ein Schritt beim Erstellen bzw. Ändern von Filtern.

Siehe "Erstellen oder Ändern von Filtern" auf Seite 370.

So aktualisieren Sie die Mitgliedschaft eines Filters

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Filter".
2. Klicken Sie im linken Bereich auf den Filter, dessen Mitgliedschaft Sie aktualisieren möchten.
3. Führen Sie im rechten Teilfenster im Bereich "Filtermitgliedschaft" eine der folgenden Optionen aus:

So aktualisieren Sie die Filtermitgliedschaft sofort	Klicken Sie auf "Mitgliedschaft aktualisieren".
So aktualisieren Sie die Filtermitgliedschaft mithilfe der Zeitpläne für die Filteraktualisierung	Klicken Sie auf "Mitgliedschaft aktualisieren"> "Automatisch".
So erlauben Sie nur manuelle Filtermitgliedschaftsaktualisierungen	Klicken Sie auf "Mitgliedschaft aktualisieren"> "Manuell". Durch diese Option werden die geplanten Aktualisierungen der Filtermitgliedschaft deaktiviert. Der Filter enthält beispielsweise eine komplexe Abfrage, die Sie nur bei Bedarf ausführen möchten.

Durchführen von Aktionen für Filterressourcen

Sie können Aktionen für ausgewählte Filterressourcen Durchführen. Diese Optionen entsprechen den Optionen im Kontextmenü (Rechtsklick). Die verfügbaren Aktionen hängen vom ausgewählten Ressourcentyp ab, d.h. einige Optionen sind möglicherweise nicht für alle Ressourcen verfügbar.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

So führen Sie eine Aktion für eine Filterressource durch

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Filter".
2. Klicken Sie im linken Bereich auf den Filter, den Sie verwenden möchten.

3 Wählen Sie im rechten Teilfenster im Bereich "Filtermitgliedschaft" die Ressource aus, für die Sie eine Aktion durchführen möchten.

4 Klicken Sie auf "Aktionen" und klicken Sie anschließend auf die entsprechende Option.

Ressourcenmanager	Öffnet die Ressource in der Ressourcenmanager-Konsole.
Exportieren	Exportiert die Ressource in eine XML-Datei.
Eigenschaften	Zeigt die Eigenschaften der Ressource an.
Asset-Status einstellen > Aktiv	Stellt den Status eines Assets auf "Aktiv". Diese Einstellung ist relevant für Asset Solution.
Asset-Status einstellen > Stillgelegt	Stellt den Status eines Assets auf "Stillgelegt". Diese Einstellung ist relevant für Asset Solution.
Einer Organisationsgruppe hinzufügen	Weisen Sie die Ressource einer Organisationsgruppe zu.
Löschen	Löschen Sie die Ressource aus dem Filter.
Energieverwaltungsaufgabe	Planen Sie die Energieverwaltungsaufgabe oder führen Sie sie aus.

Anzeigen von Filterabhängigkeiten

Bevor Sie einen Filter ändern, sollten Sie ermitteln, welche anderen Elemente davon abhängen. Sie können eine Liste aller Filter, Ziele, Aufgaben und Richtlinien anzeigen, die einen bestimmten Filter verwenden.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Die Liste der Abhängigkeiten enthält alle Ziele, die den angegebenen Filter direkt oder in einem enthaltenen Filter enthalten. Die Liste enthält auch alle Richtlinien und Aufgaben im Hinblick auf diese Ziele. Der Einschluss des Filters im Ziel führt zu einer Abhängigkeit. Die Abhängigkeit bedeutet nicht unbedingt, dass sich die Richtlinie oder Aufgabe derzeit auf eine Ressource im Filter bezieht.

So zeigen Sie die Abhängigkeiten eines Filters an

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Filter".
2. Klicken Sie im linken Teilfenster auf den Filter, für den Sie die Abhängigkeiten anzeigen möchten.
3. Klicken Sie im rechten Teilfenster im Bereich "Filtermitgliedschaft" auf "Referenziert durch".
4. Zeigen Sie im Dialogfeld "Für diesen Filter geltende Elemente" eine Liste der Filter, Ziele, Aufgaben und Richtlinien an, die den Filter verwenden.
5. Klicken Sie auf "Schließen".

Info zu Ressourcenzielen

Ein Ressourcenziel, normalerweise einfach als Ziel bezeichnet, ist eine Umgebung, in der Aufgaben und Richtlinien auf eine dynamische Ressourcensammlung angewendet werden können. Ein Ziel besteht aus mindestens einer Organisationsansicht oder -gruppe und mehreren Filtern. Die Filter dienen dazu, aus den verfügbaren Ressourcen die benötigten Ressourcen herauszusuchen. Die Organisationsansicht oder -gruppe dient als Sicherheitsfilter. Er stellt sicher, dass die Richtlinie oder Aufgabe nur auf Ressourcen angewendet wird, für die die Sicherheitsrolle des Benutzers eine Berechtigung zur Zusammenarbeit hat.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

Ziele werden in CMDB zwischengespeichert und dynamisch ausgewertet, wenn die Aufgabe oder Richtlinie ausgeführt wird. Das Ziel wird im Hinblick auf den Bereich des aktuellen Benutzers ausgewertet. Nur die Ressourcen, die in der Organisationsansicht oder -gruppe und in den Filtern erscheinen, werden zurückgegeben. Das Ziel umfasst nur die Ressourcen, für die der Benutzer Lesezugriff hat. Ressourcen außerhalb des Bereichs des aktuellen Benutzers sind nie sichtbar.

Die Systemfilter, die mit Notification Server geliefert werden, enthalten nur verwaltete Ressourcen, aber Ziele und Organisationsansichten bzw. -gruppen können nicht verwaltete Ressourcen enthalten. Sie können auch Ihre eigenen benutzerdefinierten Filter erstellen, die nicht verwaltete Ressourcen einschließen. Wenn Sie jedoch ein Ziel auf eine Richtlinie oder Aufgabe anwenden, können nur die verwalteten Computer im Ziel die Richtlinie anfordern oder die Aufgabe ausführen.

Es gibt zwei Typen von Zielen, die Sie auf eine Richtlinie oder Aufgabe anwenden können:

Automatisch generierte Ressourcenziele	Dies sind Ziele, die nicht ausdrücklich benannt und gespeichert wurden. Automatisch generierte Ziele werden nur durch die Richtlinie oder Aufgabe verwendet, in der/denen Sie sie erstellen. Beispiel: Wenn Sie die Option "Schnellzuordnung" verwenden, um einen Filter auszuwählen, oder das Dialogfeld "Ressourcen auswählen", um Ressourcensätze auszuwählen, wird das entsprechende Ziel erstellt und zur Richtlinie oder Aufgabe hinzugefügt. Das automatisch generierte Ziel erhält einen Standardnamen, der auf der Organisationsgruppe, dem Filter oder den Ressourcensätzen basiert, die darin enthalten sind. Sie können diese Ziele bearbeiten, wenn Sie die Richtlinie oder Aufgabe ändern, aber Sie können sie nicht auf alle anderen Richtlinien oder Aufgaben anwenden.
Benannte Ressourcenziele	Dies sind Ziele, die ausdrücklich als benannte Ressourcenziele gespeichert wurden. Benannte Ziele können auf eine beliebige Anzahl von Aufgaben und Richtlinien angewendet und von jedem Benutzer geändert werden, der über die entsprechenden Berechtigungen verfügt.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Siehe "Erstellen oder Ändern von Filtern" auf Seite 370.

Planen von Ressourcen-Mitgliedschaftsaktualisierungen

Sie können alle Ihre Ressourcenfilter, Organisationsgruppen und Ressourcenziele auf dem aktuellen Stand halten, indem Sie die entsprechenden Zeitpläne für die Filteraktualisierung konfigurieren. Anhand dieser Zeitpläne können Sie Filter, Organisationsgruppen und Ziele aktualisieren, die Sie in geeigneten Intervallen benötigen. Diese Zeitpläne unterstützen Sie beim Verwalten der Verarbeitungslast für Notification Server.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Vordefinierte Zeitpläne für die Ressourcen-Mitgliedschaftsaktualisierung werden in Symantec Management-Plattform bereitgestellt. Diese Zeitpläne sind für die meiste Zwecke geeignet, und Sie sollten sie nicht ändern müssen. Wenn sich jedoch die Anforderungen Ihrer Organisation ändern, können Sie die notwendigen Änderungen vornehmen.

Tabelle 23-2 Zeitpläne für die Ressourcen-Mitgliedschaftsaktualisierung

Zeitplan	Beschreibung
Delta-Aktualisierungs-zeitplan	Aktualisiert die Mitgliedschaft von Folgendem: ■ Filter, deren Mitgliedschaft seit der letzten Aktualisierung geändert wurde. ■ Alle dynamischen Organisationsgruppen. ■ Alle ungültigen Ziele. Ein Ziel kann durch die folgenden Ereignisse ungültig werden: ■ Seine Definition wird gespeichert. ■ Die Mitgliedschaft eines Filters, der es verwendet, ändert sich. ■ Die Mitgliedschaft einer Organisationsgruppe, die es verwendet, ändert sich. ■ Die Sicherheit ändert sich, die auf eine Organisationsgruppe, die es verwendet, angewendet wird. Standardmäßig wird dieser Zeitplan alle fünf Minuten ausgeführt.
Aktualisierungszeitplan fertig stellen	Dadurch wird die Mitgliedschaft aller Filter, Organisationsgruppen und Ziele unabhängig von Inventarstatus oder von Änderungen an Richtlinien komplett neu erstellt. Die vollständige Aktualisierung hat unter Umständen eine beträchtliche Last für Notification Server zur Folge und sollte dementsprechend geplant werden. Standardmäßig wird dieser Zeitplan einmal täglich ausgeführt.
Richtlinien-aktualisierungs-zeitplan	Aktualisiert die Mitgliedschaft der Filter, die eine Richtlinie verwendet, wenn sich die Richtlinie seit der letzten Aktualisierung geändert hat. Durch diesen Zeitplan wird sichergestellt, dass beim Aktualisieren oder Erstellen einer Richtlinie alle Filter, die in den neuen oder geänderten Richtlinienzielen enthalten sind, automatisch aktualisiert werden. Standardmäßig wird dieser Zeitplan alle fünf Minuten ausgeführt.

Siehe "Komponenten eines Symantec Management-Plattform-Zeitplans" auf Seite 125.

Siehe "Anzeigen des internen Zeitplankalenders des Notification Servers" auf Seite 130.

So konfigurieren Sie Zeitpläne für Ressourcen-Mitgliedschaftsaktualisierungen

1. Klicken Sie in Symantec Management Console im Menü "Einstellungen" auf "Notification Server > Aktualisierung der Ressourcenmitgliedschaft".
2. Konfigurieren Sie auf der Seite "Aktualisierung der Ressourcenmitgliedschaft" die Aktualisierungszeitpläne, die Sie verwenden möchten.

   Siehe "Angeben von Richtlinienzeitplänen" auf Seite 404.
3. Wenn Sie einen Aktualisierungszeitplan sofort ausführen möchten, klicken Sie im entsprechenden Fenster auf "Ausführen".

   Beispielsweise können Sie sicherstellen, dass alle Änderungen an Ihren Filtern sofort angewendet werden, statt bis zur geplanten Aktualisierung zu warten.
4. Klicken Sie auf "OK".

Kapitel 24

Konfigurieren von Paketen

In diesem Kapitel werden folgende Themen behandelt:

- Ändern der Konfigurationseinstellungen für ein Paket
- Aktualisieren der Verteilungspunkte für ein Paket
- Aktivieren des Zugriffs auf Pakete in einem UNC-Quellverzeichnis
- Verwalten von Paketprogrammen

Ändern der Konfigurationseinstellungen für ein Paket

Ein Paket enthält einen Satz Dateien, der an eine verwaltete Ressource geliefert werden kann. Beispielsweise enthalt das Symantec Management-Agent-Paket die Datei "AeXClientUpgrade.exe". Die Datei "AeXClientUpgrade.exe" installiert den Agent auf verwalteten Ressourcen.

Auf der Seite "Paket" können Sie die Paketeinstellungen (z. B.Paketquelle, Paketspeicherort und wie das Paket ausgeführt wird) konfigurieren.

So ändern Sie die Konfigurationseinstellungen für ein Paket

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Wählen Sie im linken Teilfenster das Paket aus, das Sie bearbeiten möchten.

3 Ändern Sie auf der Seite "Paket" die erforderlichen Konfigurationseinstellungen auf den entsprechenden Registerkarten:

Paket	
Programme	Siehe "Verwalten von Paketprogrammen" auf Seite 390.
Package Server	
Erweitert	

4 Klicken Sie auf "Änderungen speichern", um die neuen Einstellungen zu bestätigen.

Sie müssen die Paketverteilungspunkte aktualisieren, um die Paketinformationen auf dem jeweiligen Package Server zu aktualisieren.

Siehe "Aktualisieren der Verteilungspunkte für ein Paket" auf Seite 388.

Aktualisieren der Verteilungspunkte für ein Paket

Paketverteilungspunkte sind die Speicherorte, in denen das Paket gespeichert wird, zum Beispiel Package Server oder UNC-Quellorte. Mit jedem Paket wird eine XML-Datei gespeichert, die Informationen über das jeweilige Paket enthält. Diese Informationen müssen bei jeder Paketänderung aktualisiert werden. Notification Server und Package Server verwenden diese Informationen, um bei Paketanforderungen verwalteter Computer die passenden Dateien zu liefern. Die Paketinformationen werden nach einem Zeitplan aktualisiert. Bei Bedarf kann jedoch auch eine manuelle Aktualisierung veranlasst werden. Beispielsweise können Sie die Verteilungspunkte manuell aktualisieren, damit ein geändertes Paket sofort die Paketinformationen über alle seine Verteilungspunkte aktualisiert.

Siehe "Ändern der Konfigurationseinstellungen für ein Paket" auf Seite 387.

Sie können Verteilungspunkte für ein Paket im Softwarekatalog oder für ein Paket aktualisieren, auf das vom Menü "Einstellungen" aus zugegriffen wird.

So aktualisieren Sie die Paketverteilungpunkte für ein Paket im Softwarekatalog

1 Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Softwarekatalog".

2 Führen Sie im Fenster "Softwarekatalog" einen der folgenden Schritte aus:

- Wählen Sie bei einer nicht definierten Softwarekomponente diese in der Liste "Neu erkannte bzw. nicht definierte Software" aus und klicken Sie auf das Symbol "Bearbeiten". Befindet sich die nicht definierte

Softwarekomponente nicht in der Liste, klicken Sie unten in der Liste auf "Gesamte Software anzeigen".

- Suchen Sie bei einer definierten Softwarekomponente das Softwareprodukt, mit dem die Softwarekomponente verknüpft ist, in der Liste "Verwaltete Softwareprodukte" oder "Nicht verwaltete Software". Klicken Sie anschließend auf das Plus -Zeichen vor dem Softwareprodukt und dann auf den Link für die Softwarekomponente, der unterhalb des Softwareprodukts angezeigt wird.

3 Klicken Sie auf der Seite "Softwareressource" auf der Registerkarte Paket im Fenster Pakete auf das Paket, dessen Verteilungspunkte Sie aktualisieren möchten.

4 Klicken Sie auf Aktionen > Verteilungspunkte aktualisieren.

So aktualisieren Sie die Paketverteilungpunkte für ein Paket über das Menü "Einstellungen"

1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".

2 Wählen Sie im linken Teilfenster das Paket aus, dessen Verteilungspunkte Sie aktualisieren möchten.

3 Klicken Sie unten auf der Seite "Paket" auf "Verteilungspunkte aktualisieren".

Aktivieren des Zugriffs auf Pakete in einem UNC-Quellverzeichnis

Der Symantec Management-Agent verwendet die Agent-Authentifizierungsinformationen (ACC), um zum IIS auf dem Notification Server eine Verbindung herzustellen, um UNC-Pakete über HTTP herunterzuladen. IIS authentifiziert sich dann mithilfe der Verteilungspunkt-Identifikationsdaten (DPC) gegenüber der UNC-Quelle. Der Symantec Management-Agent verwendet die ACC, um eine Verbindung zum Herunterladen von Quellen herzustellen. Stellen Sie sicher, dass die ACC Lesezugriff haben, wenn der Symantec Management-Agent direkt aus der UNC-Paketquelle herunterlädt.

Die DPC werden nicht verwendet, wenn der Symantec Management-Agent ein Paket von einem Package Server herunterlädt. Der Package Server weist den heruntergeladenen Paketdateien entweder anonymen Zugriff oder die ACC zu.

So aktivieren Sie den Zugriff auf Pakete in einem UNC-Quellverzeichnis

1. Geben Sie die Paketverteilungpunktidentifikationsdaten an, die Sie verwenden möchten.

   Sie geben diese Identifikationsdaten auf der Seite "Notification Server-Einstellungen" auf der Registerkarte "Verteilungspunkt-Identifikationsdaten" an. Sie sollten beim Festlegen der Paketverteilungspunkt-Identifikationsdaten die Option "Agent-Authentifizierungsinformationen verwenden" auswählen. Damit wird sicher gestellt, dass nur eine Art von Identifikationsdaten, nämlich die Agent-Authentifizierungsinformationen, in den UNC-Paketverzeichnissen vorliegen müssen.

   Siehe "Einstellungen für Verteilungspunkt-Identifikationsdaten" auf Seite 76.

2. Gewähren Sie über diese Identifikationsdaten Lesezugriff auf den UNC-Quellordner.

Verwalten von Paketprogrammen

Ein Paket kann aus mehr als einem Programm bestehen. Sie können die Programme in einem Paket Ihren Anforderungen entsprechend verwalten. Sie können Programmdetails ändern, neue Programme dem Paket hinzufügen und alle Programme löschen, die Sie nicht mehr benötigen.

Siehe "Ändern der Konfigurationseinstellungen für ein Paket" auf Seite 387.

So zeigen Sie Details eines Paketprogramms an

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Wählen Sie im linken Teilfenster das Paket aus, das Sie bearbeiten möchten.
3. Wählen Sie auf der Seite "Paket" auf der Registerkarte "Programme", das Programm aus, das Sie anzeigen möchten

So erstellen Sie ein neues Paketprogramm

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Wählen Sie im linken Teilfenster das Paket aus, das Sie bearbeiten möchten.
3. Klicken Sie auf der Seite "Paket" auf der Registerkarte "Programme" auf "Neu".
4. Geben Sie die Programmdetails in den entsprechenden Feldern an.
5. Klicken Sie auf "Übernehmen".

So entfernen Sie ein Programm aus einem Paket

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Wählen Sie im linken Teilfenster das Paket aus, das Sie bearbeiten möchten.
3. Wählen Sie auf der Seite "Paket" auf der Registerkarte "Programme" das Programm aus, das Sie entfernen möchten, und klicken Sie anschließend auf "Löschen".
4. Klicken Sie auf "Übernehmen".

Kapitel 25

Verwenden von Richtlinien

In diesem Kapitel werden folgende Themen behandelt:

- Informationen zu Symantec Management-Plattform-Richtlinien
- Infos zu benutzerbasierten Richtlinien
- Verwalten von Symantec Management-Plattform-Richtlinien
- Anwenden eine Richtlinie mit Drag and Drop
- Festlegen der Ziele für Richtlinien oder Aufgaben
- Ändern eines Ressourcenziels
- Erstellen eines Ressourcenziels
- Auswählen eines vorhandenen Ressourcenziels
- Speichern eines benannten Ressourcenziels
- Angeben von Filterregeln für Ressourcenziele
- Auswählen benannter Ressourcenziele
- Angeben von Richtlinienzeitplänen
- Konfigurieren der Installations-, Aktualisierungs- und Deinstallationsrichtlinien für Agents und Plugins
- Infos zu Automatisierungsrichtlinien
- Schlüsselkomponenten von Automatisierungsrichtlinien
- Verwalten von Automatisierungsrichtlinien
- Erstellen und Ändern von geplanten Automatisierungsrichtlinien
- Erstellen und Ändern von meldungsbasierten Automatisierungsrichtlinien

- Erstellen und Ändern von Automatisierungsrichtlinien-Aufgaben

Informationen zu Symantec Management-Plattform-Richtlinien

Bei der Symantec Management-Plattform-Richtlinie handelt es sich um einen Satz von Regeln, die sich auf eine Ressource oder einen Satz von Ressourcen beziehen (bekannt als das Richtlinienziel). Eine Richtlinie kann basierend auf einem Zeitplan oder auf eingehenden Daten ausgewertet werden. Wenn eine Richtlinie ausgewertet wird, wird die entsprechende Aktion vorgenommen. Diese Aktion enthält im Allgemeinen ausgeführte Aufgaben auf den Zielressourcen, um sicherzustellen, dass sie alle der Richtlinie entsprechen.

Tabelle 25-1 Allgemeine Symantec Management-Plattform-Richtlinientypen

Richtlinientyp	Beschreibung
Agent	Gibt die Symantec Management-Agent-Konfigurationseinstellungen auf Clientcomputern an. Siehe "Konfigurieren des Symantec Management-Agent" auf Seite 288.
Automatisierung	Gibt automatisierte Aktionen an, die auf Clientcomputern oder dem Notification Server-Computer durchgeführt werden sollen. Diese Richtlinien sind dynamisch. Sie zielen auf die entsprechenden Computer an, wenn die Richtlinie aktiviert wird, und führen die je nach aktuellem Zustand des jeweiligen Zielcomputers erforderlichen Aktionen durch. Automatisierungsrichtlinienziele können auf Berichtergebnissen oder einer Abfrage statt wie bei anderen Richtlinientypen auf Filter und Ressourcenziele basiert sein. Siehe "Infos zu Automatisierungsrichtlinien" auf Seite 408.
Benutzer	Gibt die Einstellungen an, die für bestimmte Benutzer gelten. Diese Einstellungen werden auf die Computer angewendet, an denen die Benutzer eingeloggt sind. Siehe "Infos zu benutzerbasierten Richtlinien" auf Seite 394.
Lösung	Lösungen können ihre eigenen Richtlinien bereitstellen, die auf Computer oder Benutzer jener Lösungen abzielen.

Infos zu benutzerbasierten Richtlinien

Benutzerbasierte Richtlinien können auf bestimmte Benutzer oder Benutzergruppen angewendet werden. Sie können ggf. auch auf bestimmte Computer angewendet werden.

Siehe "Informationen zu Symantec Management-Plattform-Richtlinien" auf Seite 393.

Einige Organisationen haben z. B. eine große Anzahl von Active Directory-Sicherheitsgruppen und müssen deren Richtlinien mittels dieser Sicherheitsgruppen anwenden. Die Sicherheitsgruppen, die verwaltete Computer oder Benutzer enthalten, werden in die CMDB importiert. Der Einsatz benutzerbasierter Richtlinien ermöglicht es dem Administrator, Computer mithilfe der vorhandenen Active Directory-Infrastruktur zu verwalten. Arbeitsgruppen und lokale Benutzer werden unterstützt.

Benutzerbasierte Richtlinien werden nur angewendet, wenn der Benutzer an einem verwalteten Computer angemeldet ist. Diese Richtlinien werden nur für den Benutzer angewendet, der an der Konsolensitzung angemeldet ist. Jedes Mal, wenn sich ein Benutzer an einem verwalteten Computer anmeldet, sucht Symantec Management-Agent nach den benutzerbasierten Richtlinien, die Anwendung auf den Benutzer finden. Richtlinien werden auf dem Computer für den Zeitraum von einer Woche zwischengespeichert. Der Symantec Management-Agent stellt außerdem regelmäßige Konfigurationsanfragen für aktive Richtlinien, die die SID des aktuell angemeldeten Benutzer verwenden. Das geschieht zusätzlich zur GUID des verwalteten Computers, sodass sowohl benutzer- als auch computerbasierte Richtlinien Anwendung finden. Der Agent stellt diese Anfrage, wenn sich ein Benutzer zum ersten Mal an einem verwalteten Computer einloggt. Der Agent wiederholt die Anfrage jedes Mal, wenn die normale Konfigurationsanfrage durchgeführt wird.

Hinweis: Benutzer, die über Terminaldienste an verwalteten Computern angemeldet sind, erhalten keine auf sie abgezielten Richtlinien. Alle Benutzer sehen die Richtlinien, die für den Benutzer angewendet werden, der an die Konsolensitzung angemeldet ist.

Es mag sinnvoll sein, einige Computer oder Benutzer von benutzerbasierten Richtlinien auszuschließen. Beispiel: Ein verwalteter Computer, der von vielen Benutzern gemeinsam genutzt wird, oder ein Administrator, der sich jeden Tag bei vielen verschiedenen Computern einloggt. Wenn ein derartiger Computer oder Benutzer Ziel einer benutzerbasierten Richtlinie ist, können die häufigen von Richtlinien gesteuerten Änderungen erhebliche Belastungen der betroffenen Computer bedeuten.

Sie können eine Liste von Computern erstellen, auf die benutzerbasierte Richtlinien nicht zutreffen. Sie können eine Liste von Benutzern erstellen, auf die benutzerbasierte Richtlinien nicht angewendet werden sollen. Sie können diese Listen als Ausschlüsse in den entsprechenden Filtern verwenden.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Siehe "Erstellen oder Ändern von Filtern" auf Seite 370.

Verwalten von Symantec Management-Plattform-Richtlinien

Die Ansicht "Richtlinien" zeigt alle verfügbaren Richtlinien in einer einzelnen Ordnerstruktur an. Diese Standardstruktur ermöglicht einfachen Zugriff auf die Richtlinien, um Sie anzuzeigen oder zu ändern.

Siehe "Informationen zu Symantec Management-Plattform-Richtlinien" auf Seite 393.

Siehe "Infos zu Automatisierungsrichtlinien" auf Seite 408.

So verwalten Sie Richtlinien

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Richtlinien".
2. Wählen Sie im linken Bereich unter dem Ordner "Richtlinien" die zu verwaltende Richtlinie oder Richtliniengruppe aus.

Anwenden eine Richtlinie mit Drag and Drop

In der Ansicht "Richtlinien" können Sie nach Richtlinien suchen, sie anzeigen und anwenden. Diese erweiterte Ansicht verfügt über ein Suchfeld, über das Sie schnell die Richtlinien finden, mit denen Sie arbeiten möchten. Sie können nach Richtlinienname oder -typ suchen.

Siehe "Informationen zur Ansicht Richtlinien " auf Seite 44.

Sie können Richtlinien starten, indem Sie sie per Drag and Drop auf einen oder mehrere Computer ziehen. Sie können auch die Option "Schnellzuordnung" verwenden, um eine Richtlinie ohne einen manuellen Drilldown zu bearbeiten.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

Hinweis: Eine der folgenden Lösungen oder Suites muss installiert sein, damit diese Aufgabe ausgeführt wird: Deployment Solution (eigenständiges Produkt), IT Management Suite, Server Management Suite oder Client Management Suite.

So wenden Sie eine Richtlinie per Drag and Drop an

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Richtlinien".
2. Klicken Sie im Navigationsbereich auf die Richtlinie, die Sie ausführen möchten, und ziehen Sie sie nach rechts, um den Drag & Drop-Vorgang zu initiieren.

   Die Ergebnisse Ihrer aktuellsten Computersuche erscheinen im Listenbereich. Wenn Sie Ihre letzte Computersuche gefiltert haben, werden die Ergebnisse der gefilterten Suche in der Liste angezeigt.

   Siehe "Suchen nach einem Computer und Speichern der Suche als Filter" auf Seite 39.
3. Um die Computer zu auswählen, auf denen Sie die Richtlinie ausführen möchten, führen Sie eine der folgenden Schritte aus:
   - Um die Richtlinie auf allen aufgeführten Computern auszuführen, legen Sie sie auf das Namenssymbol im Listenbereich ab.
   - Um die Richtlinie auf einem bestimmten Computer auszuführen, legen Sie sie auf dem Computer in der Liste ab.
   - Um die Richtlinie auf einer gespeicherten Suche, Organisationsansicht oder Organisationsgruppe auszuführen, ziehen Sie sie auf die Blade "Computer" und legen Sie sie dann auf eine gespeicherte Suche, eine Organisationsansicht oder eine Organisationsgruppe ab.
4. Klicken Sie im Dialogfeld "Richtlinie anwenden" auf "OK".

Festlegen der Ziele für Richtlinien oder Aufgaben

Sie müssen ein oder mehrere Ziele für eine Richtlinie oder Aufgabe festlegen. Ein Ziel definiert die Computer, Benutzer und Ressourcen, auf die die Richtlinie oder Aufgabe angewendet wird. Eine Richtlinie oder Aufgabe kann über mehrere Ziele verfügen.

Sie können die folgenden Typen von Zielen auf eine Richtlinie oder Aufgabe anwenden:

Automatisch generierte Ressourcenziele	Diese Ziele wurden nicht ausdrücklich benannt und gespeichert. Automatisch generierte Ziele werden nur durch die Richtlinie oder Aufgabe verwendet, in der/denen Sie sie erstellen. Sie können diese Ziele bearbeiten, wenn Sie die Richtlinie oder Aufgabe ändern, aber Sie können sie nicht auf alle anderen Richtlinien oder Aufgaben anwenden.

Benannte Ressourcenziele	Diese Ziele wurden ausdrücklich als benannte Ressourcenziele gespeichert. Benannte Ziele können auf eine beliebige Anzahl von Aufgaben und Richtlinien angewendet und von jedem Benutzer geändert werden, der über die entsprechenden Berechtigungen verfügt. Siehe "Speichern eines benannten Ressourcenziels" auf Seite 400.

Ziele werden in Symantec Management Console nicht als Elemente aufgeführt. Jedoch können Sie mit der Option "Schnellzuordnung" vorhandene benannte Ziele auswählen, die auf eine Richtlinie oder Aufgabe angewendet werden sollen. Sie können auch die Liste der verfügbaren benannten Ziele im Dialogfeld "Speichern unter" anzeigen, wenn Sie ein benanntes Ziel erstellen oder ändern.

Siehe "Info zu Ressourcenzielen" auf Seite 383.

So geben Sie das Ziel einer Richtlinie oder Aufgabe an

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Richtlinien".
2. Wählen Sie im linken Bereich unter dem Ordner "Richtlinien" die zu verwaltende Richtlinie oder Richtliniengruppe aus.
3. Klicken Sie auf der Seite *"Richtlinienname"* oder *"Aufgabenname"* unter "Gilt für/Richtlinieneinhaltung" auf "Zuordnen zu" und dann auf eine der folgenden Optionen:

Schnellzuordnung	1. Wählen Sie in der Dropdown-Liste im Dialogfeld "Schnellzuordnung" das entsprechende benannte Ziel, die Organisationsgruppe oder den Filter aus. 2. (Optional) Geben Sie die ersten Buchstaben des gewünschten Elements ein. Die Optionen auf der Liste werden auf die passenden Angaben reduziert. 3. Klicken Sie auf "Übernehmen".
Computer	Wählen Sie im Fenster "Computer auswählen" die gewünschten Computer aus. Siehe "Erstellen eines Ressourcenziels" auf Seite 399.
Benutzer	Wählen Sie im Fenster "Benutzer auswählen" die gewünschten Benutzer aus. Siehe "Erstellen eines Ressourcenziels" auf Seite 399.

Ressourcen	Wählen Sie im Fenster "Ressourcen auswählen" die gewünschten Ressourcen aus. Siehe "Erstellen eines Ressourcenziels" auf Seite 399.

Beachten Sie, dass einige Optionen möglicherweise nicht für alle Richtlinien verfügbar sind.

Jede Auswahl wird zur Liste der Ziele im Raster "Anwenden auf" hinzugefügt.

Wiederholen Sie diesen Schritt, um beliebig viele Ziele hinzuzufügen.

4 (Optional) Klicken Sie in der Dropdown-Liste "Ansicht" auf die entsprechende Option: "Computer und Benutzer", "Angewandt von" oder "Aufgabenausführungen".

In der Liste werden nur die Elemente angezeigt, die ausdrücklich ausgewählt wurden. Wenn Sie z. B. Computer anzeigen, können Sie nur die Computer sehen, die Sie im Dialogfeld "Computer auswählen" ausgewählt haben. Es werden keine zusätzlichen Computer angezeigt, die in den Zielen enthalten sind, die Sie im im Dialogfeld "Schnellzuordnung" ausgewählt haben.

5 Wenn Sie ein Ziel ändern oder es aus der Liste löschen möchten, wählen Sie es im Raster "Gilt für/Richtlinieneinhaltung" aus, und klicken Sie anschließend je nach Wunsch auf "Bearbeiten" oder "Löschen".

Siehe "Ändern eines Ressourcenziels" auf Seite 398.

6 Klicken Sie auf "Änderungen speichern".

Ändern eines Ressourcenziels

Wenn Sie eine Richtlinie oder Aufgabe ändern, können Sie alle darin enthaltenen automatisch generierten Ziele und alle benannten Ressourcenziele ändern, auf die Sie Zugriff haben.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

Siehe "Verwalten von Symantec Management-Plattform-Richtlinien" auf Seite 395.

So ändern Sie ein Ressourcenziel

1 Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Richtlinien".

2 Wählen Sie im linken Bereich unter dem Ordner "Richtlinien" die zu verwaltende Richtlinie oder Richtliniengruppe aus.

3. Klicken Sie auf der Seite *"Richtlinienname"* oder *"Aufgabenname"* im Teilfenster "Gilt für/Richtlinieneinhaltung" in der Dropdown-Liste "Ansicht" auf "Computer und Benutzer".
4. Wählen Sie im Raster "Gilt für/Richtlinieneinhaltung" das Ziel aus, das Sie ändern möchten.
5. Klicken Sie auf "Bearbeiten".
6. Nehmen Sie im Fenster "Ausgewählte Gruppe bearbeiten" die notwendigen Änderungen am Ziel vor.

   Siehe "Erstellen eines Ressourcenziels" auf Seite 399.

Erstellen eines Ressourcenziels

In den Dialogfeldern "Computer auswählen", "Benutzer auswählen" und "Ressourcen auswählen" können Sie die Elemente auswählen, die Sie in einem neuen Ressourcenziel einschließen möchten. Im Dialogfeld "Ausgewählte Gruppe bearbeiten" können Sie die Auswahl für ein vorhandenes Ressourcenziel ändern.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

So erstellen Sie ein Ressourcenziel

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Richtlinien".
2. Wählen Sie im linken Bereich unter dem Ordner "Richtlinien" die zu verwaltende Richtlinie oder Richtliniengruppe aus.
3. Doppelklicken Sie auf der Seite *"Richtlinienname"* oder *"Aufgabenname"* im Bereich "Gilt für/Richtlinieneinhaltung" auf die Ressource, die Sie verwalten möchten.
4. Wenn Sie für das Ressourcenziel ein bestimmtes vorhandenes Ziel als Grundlage verwenden möchten, klicken Sie im Dialogfeld "Ziel hinzufügen" auf "Öffnen" und dann im Fenster "Öffnen" auf das entsprechende Ziel.

   Siehe "Auswählen eines vorhandenen Ressourcenziels" auf Seite 400.
5. Geben Sie unter "Filterregeln" die Regeln an, nach denen Sie die verfügbaren Computer, Benutzer oder Ressourcen filtern möchten.

   Siehe "Angeben von Filterregeln für Ressourcenziele" auf Seite 401.

6 Wenn Sie das Ressourcenziel als benanntes Ziel speichern möchten, klicken Sie auf "Speichern unter".

Siehe "Speichern eines benannten Ressourcenziels" auf Seite 400.

7 Wenn die Liste (Elemente), die zurzeit mit Regeln übereinstimmen: die von Ihnen gewünschten Elemente anzeigt, klicken Sie auf "OK".

Das angegebene Ressourcenziel wird zur Richtlinie oder Aufgabe hinzugefügt. Wenn das Ziel automatisch erstellt wird (wurde nicht als benanntes Ziel gespeichert), erhält es einen Standardnamen, der auf den Namen der Organisationsgruppen und Filter basiert, die es benutzt.

Auswählen eines vorhandenen Ressourcenziels

Im Dialogfeld "Öffnen" können Sie ein vorhandenes benanntes Ressourcenziel oder eine benannte Gruppe von Ressourcenzielen (die selbst ein Ressourcenziel ist) auswählen. Wenn Sie über die Ressourcenzielerstellung (im Allgemeinen das Fenster "Ressourcen auswählen") oder die Ressourcenzielauswahl (im Allgemeinen das Fenster "Ressourcenziel auswählen" oder "Eine Gruppe auswählen") auf dieses Dialogfeld zugreifen, ersetzt das Ziel oder die Gruppe von Zielen, das/die Sie ausgewählt haben, die aktuelle Auswahl im Fenster. Wenn Sie über das Ressourcenauswahlfenster ("Computer auswählen" oder "Ressourcen auswählen") auf dieses Dialogfeld zugreifen, wird die Zielmitgliedschaft zur aktuellen Auswahl im Fenster hinzugefügt.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

Siehe "Speichern eines benannten Ressourcenziels" auf Seite 400.

So wählen Sie ein vorhandenes Ressourcenziel aus

1 Klicken Sie im Dialogfeld "Computer/Ressourcen auswählen", "Eine Gruppe auswählen" oder "Ausgewählte Gruppe bearbeiten" auf "Öffnen".

2 Klicken Sie im Dialogfeld "Öffnen" in der Liste der benannten Ressourcenziele oder -gruppen auf das passende Ziel oder die passende Gruppe.

3 Klicken Sie auf "OK".

Speichern eines benannten Ressourcenziels

Wenn Sie ein Ressourcenziel in mehreren Aufgaben und Richtlinien verwenden oder es anderen Benutzern zur Verfügung stellen möchten, können Sie das Ziel als benanntes Ressourcenziel speichern. Benannte Ziele können auf eine beliebige Anzahl von Aufgaben und Richtlinien angewendet werden. Jeder Benutzer, der die entsprechenden Berechtigungen hat, kann auf von Ihnen erstellte benannte Ziele

zugreifen oder sie ändern. Sie können auch benannte Gruppen von Ressourcenzielen, falls geeignet, speichern, beispielsweise für den Einschluss in Replizierungsregeln.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

Siehe "Auswählen benannter Ressourcenziele" auf Seite 403.

Siehe "Auswählen eines vorhandenen Ressourcenziels" auf Seite 400.

Wenn Sie auf das Fenster "Speichern unter" über die Ressourcenzielauswahl (im Allgemeinen die Fenster "Ressourcenziel auswählen" oder "Eine Gruppe auswählen") zugreifen, können Sie die ausgewählten Ressourcenziele als benannte Gruppe von Ressourcenzielen speichern. Wenn Sie auf das Fenster "Speichern unter" über die Ressourcenzielerstellung (im Allgemeinen "Computer auswählen" oder "Ressourcen auswählen") zugreifen, können Sie die ausgewählten Ressourcen (die unter Verwendung einer Abfrage ausdrücklich angegeben oder dynamisch ausgewählt werden können) als benanntes Ressourcenziel speichern.

So speichern Sie ein benanntes Ressourcenziel

1. Klicken Sie im Dialogfeld "Computer/Ressourcen auswählen", "Eine Gruppe auswählen" oder "Ausgewählte Gruppe bearbeiten" auf "Speichern unter".
2. Führen Sie im Dialogfeld "Speichern unter" eine der folgenden Aktionen aus:

So erstellen Sie ein neues Ziel oder eine neue Gruppe	Geben Sie in das Feld "Name" den passenden Namen für das Ziel oder die Gruppe ein.
So überschreiben Sie ein vorhandenes Ziel oder eine vorhandene Gruppe	Klicken Sie in der Liste der benannten Ziele oder Gruppen auf den passenden Namen. Nur die Ziele oder Gruppen, auf die Sie Schreibzugriff haben, können ausgewählt werden. Alle schreibgeschützten Ziele oder Gruppen sind ausgegraut.

3. Klicken Sie auf "OK".

Angeben von Filterregeln für Ressourcenziele

Mit den Filterregeln können Sie Computer, Benutzer und Ressourcen filtern, um die Elemente zu identifizieren, die Sie auswählen möchten. Die Regeln werden in der Reihenfolge angewendet, in der sie aufgelistet sind, damit ausgeschlossene Elemente durch eine spätere Regel wieder eingeschlossen werden können. Die Liste der "(Elemente), die zurzeit mit den Regeln übereinstimmen" zeigt die Elemente an, die die angegebenen Regeln ausgewählt haben. Die Liste wird automatisch aktualisiert, wenn Sie Filterregeln hinzufügen und ändern.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

So legen Sie eine Filterregel fest

1. Klicken Sie im Fenster "Elemente auswählen" unter "Filterregeln" auf "Regel hinzufügen".
2. Klicken Sie in der ersten Dropdown-Liste auf den entsprechenden Vorgang:

Ausschließen der Elemente in	Schließt die im angegebenen Filter oder in der Organisationsgruppe vorhandenen Elemente oder ausgewählte Ressourcen von der Elementliste aus.
Ausschließen der Elemente nicht in	Schließt die im angegebenen Filter oder in der Organisationsgruppe nicht vorhandenen Elemente oder ausgewählte Ressourcen von der Elementliste aus.

3. Klicken Sie in der zweiten Dropdown-Liste auf die entsprechende Option:

Filtern	Wenden Sie den Vorgang auf einen bestimmten Filter an.
Gruppe	Wenden Sie den Vorgang auf eine bestimmte Organisationsgruppe an.
Elementliste	Wenden Sie den Vorgang auf angegebene Computer, Benutzer oder Ressourcen an.

4. Wählen Sie in der dritten Dropdown-Liste das entsprechende Element aus:

So wählen Sie einen Filter oder eine Gruppe aus	Geben Sie die ersten paar Buchstaben des gewünschten Filters oder der gewünschten Organisationsgruppe ein. Die Optionen auf der Liste werden auf die passenden Angaben reduziert.
So wählen Sie bestimmte Elemente aus	Klicken Sie auf die Auslassungspunkte …, und wählen Sie anschließend im Fenster "Element auswählen" die entsprechenden Elemente aus.

So verwalten Sie die Liste der Filterregeln

1. Wenn Sie eine Regel in der Liste der Filterregeln nach oben oder nach unten verschieben möchten, klicken Sie auf die Nach-oben- oder Nach-unten-Taste.
2. Wenn Sie eine Filterregel aus der Liste entfernen möchten, klicken Sie auf "Löschen".

Auswählen benannter Ressourcenziele

Im Fenster "Ressourcenziel auswählen" oder "Eine Gruppe auswählen" können Sie die benannten Ressourcenziele auswählen, die Sie benutzen möchten. Im linken Teilfenster wird die Liste verfügbarer Ressourcenziele und im rechten Teilfenster die Liste ausgewählter Ressourcenziele angezeigt.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

Sie können die ausgewählten Ressourcenziele im linken Teilfenster nach Organisationsansicht oder einer bestimmten Organisationsgruppe filtern. Der Filter schränkt die Mitgliedschaft der ausgewählten Ziele für Ressourcen ein, die in der angegebenen Organisationsansicht oder -gruppe enthalten sind. Sie können auch neue benannte Ressourcenziele erstellen.

Sie müssen die Ressourcenziele hinzufügen, die Sie für die Liste der Ressourcenziele im rechten Teilfenster auswählen möchten. Sie können die ausgewählten Ressourcenziele als benannte Gruppe von Ressourcenzielen auch speichern.

So wählen Sie benannte Ressourcenziele aus

1. (Optional) Wenn Sie die Mitgliedschaft der ausgewählte Ressourcenziele nach einer bestimmten Organisationsansicht oder -gruppe filtern möchten, wählen Sie in der Dropdown-Liste "Gruppe" die passende Organisationsansicht oder -gruppe aus.
2. (Optional) Wenn Sie ein neues benanntes Ressourcenziel erstellen möchten, klicken Sie auf "Ziel erstellen".

   Siehe "Erstellen eines Ressourcenziels" auf Seite 399.
3. Wählen Sie im linken Teilfenster die gewünschten Ressourcenziele aus, und klicken Sie dann auf >, um sie im rechten Teilfenster zur Liste der ausgewählten Ressourcenziele hinzuzufügen.
4. (Optional) Wenn Sie die in einer vorhandenen benannten Ressourcenzielgruppe enthaltenen Ressourcenziele auswählen möchten, klicken Sie auf "Öffnen" und wählen anschließend im Dialogfeld "Öffnen" die entsprechende Gruppe aus.

   Siehe "Auswählen eines vorhandenen Ressourcenziels" auf Seite 400.

   Die Ressourcenziele in der ausgewählten Gruppe werden zur Liste im rechten Teilfenster hinzugefügt.
5. (Optional) Wenn Sie Ressourcenziele aus der Liste der ausgewählten Ressourcenziele entfernen möchten, wählen Sie die passenden Ressourcenziele aus und klicken anschließend auf <.

6 (Optional) Wenn Sie die Ressourcenziele in der Liste der ausgewählten Ressourcenziele als benannte Gruppe für eine spätere Wiederverwendung speichern möchten, klicken Sie auf "Speichern unter" und geben im Dialogfeld "Speichern unter" einen passenden Namen ein.

Siehe "Speichern eines benannten Ressourcenziels" auf Seite 400.

7 Klicken Sie auf "OK".

Angeben von Richtlinienzeitplänen

Geben Sie die Zeiten an, zu denen eine Richtlinie ausgelöst wird, indem Sie den jeweiligen Zeitplan konfigurieren. Sie können so viele Zeitpläne festlegen, wie Sie möchten. Auch können beliebig viele Zeitpläne gleichzeitig aktiviert sein.

Siehe "Informationen zu Symantec Management-Plattform-Richtlinien" auf Seite 393.

Dieses Thema gilt auch für andere Zeitpläne, wie zum Beispiel bei der Aktualisierung der Ressourcenmitgliedschaft. Einige der hier beschriebenen Optionen sind möglicherweise nicht für alle Richtlinien verfügbar.

So geben Sie einen Richtlinienzeitplan an

1 Klicken Sie auf der Seite für die Richtlinie unter Zeitplan auf Zeitplan hinzufügen und dann auf eine der folgenden Optionen:

Geplante Zeit	1 Geben Sie im Feld "Start" die jeweilige Zeit an. 2 Soll der Zeitplan wiederholt werden, klicken Sie auf Wiederholen, und legen Sie im Dialogfeld Wiederholungsplan die gewünschte Häufigkeit fest.
Wartungsfenster	1 Füllen Sie die Felder für das Start- und Enddatum sowie die Dauer aus. 2 Aktivieren Sie im Fenster Dauer alle Kontrollkästchen, und geben Sie ein geeignetes Intervall an. 3 Soll der Zeitplan wiederholt werden, klicken Sie auf Wiederholen, und legen Sie im Dialogfeld Wiederholungsplan die gewünschte Häufigkeit fest.
Beim Benutzer-Login	Die Richtlinie wird ausgelöst, wenn sich ein Benutzer beim verwalteten Computer einloggt.
Beim Computerstart	Die Richtlinie wird ausgelöst, wenn der verwaltete Computer gestartet wird.

Die einzelnen Zeitpläne werden der Liste der Richtlinienzeitpläne hinzugefügt. Wiederholen Sie diesen Schritt, um weitere Zeitpläne hinzuzufügen.

2 Wählen Sie in der Dropdown-Liste "Zeitzone" die gewünschte Zeitzone aus:

Zeit des Agents verwenden	Die Zeiten werden ohne Zeitzoneninformationen angegeben und auf den verwalteten Computern der Ortszeit entsprechend angewendet. Zeitpläne werden je nach Zeitzone der verwalteten Computer zu verschiedenen Zeiten ausgeführt.
Zeit des Servers verwenden	Die Zeiten werden mit Zeitzoneninformationen angegeben. Dabei entspricht die Zeitzonenabweichung der Zeitzone des Servers, auf dem die Richtlinie definiert ist. Die Zeitpläne werden ungeachtet der Zeitzonen gleichzeitig ausgeführt. Die Sommerzeit wird berücksichtigt. Diese Option stellt sicher, dass die Zeitpläne immer anhand der auf dem Server angegebenen Ortszeit ausgerichtet werden, auf dem die Richtlinie erstellt wird.
Nach UTC koordinieren	Die Zeiten werden mit Zeitzoneninformationen angegeben, wobei die Zeitzonenabweichung 0 beträgt. Die Zeitpläne werden gleichzeitig und ungeachtet der Zeitzonen ausgeführt und sind nicht von der Sommerzeit betroffen.

3 Klicken Sie auf Erweitert, und nehmen Sie im Dialogfeld Erweiterte Optionen dann die gewünschten Änderungen vor:

Nur überprüfen, wenn:	Aktivieren Sie die entsprechenden Optionen: ■ Computer ist mit dem Netzwerk verbunden ■ Computer ist genau zum geplanten Zeitpunkt verfügbar ■ Ein Benutzer ist am Computer eingeloggt ■ Es ist kein Benutzer am Computer eingeloggt

Start-/Enddaten	Das Startdatum ist das Datum, an dem die Richtlinie in Kraft tritt. Die Richtlinie muss genauso wie andere Richtlinien aktiviert werden. Sie können die Richtlinie jederzeit vor oder nach dem Startdatum aktivieren. Wenn die Richtlinie für einen begrenzten Zeitraum verfügbar sein soll, legen Sie das Enddatum entsprechend fest. Nach diesem Datum ist die Richtlinie nicht mehr verfügbar, egal ob sie aktiviert ist oder nicht. Die Angabe eines Enddatums ist optional. Wird kein Enddatum angegeben, ist die Richtlinie zeitlich unbefristet verfügbar.

4 Klicken Sie auf OK, um das Dialogfeld Erweiterte Optionen zu schließen.

5 (Optional) Wenn Sie einen Zeitplan aus der Liste löschen möchten, wählen Sie ihn aus, und klicken Sie dann auf Löschen.

Konfigurieren der Installations-, Aktualisierungs- und Deinstallationsrichtlinien für Agents und Plugins

Sie können die Agent-Installations-, Agent-Upgrade- und Agent-Deinstallationsrichtlinien nach Ihren Anforderungen konfigurieren. Diese Richtlinien verwenden das gleiche Agent-Paket, aber jede Richtlinie verwendet ein anderes Programm.

So konfigurieren Sie Installations-, Aktualisierungs- und Deinstallationsrichtlinien für Agents und Plugins

1 Klicken Sie in der "Symantec Management Console" im Menü "Einstellungen" auf "Alle Einstellungen".

2 Erweitern Sie im linken Teilfenster den entsprechenden Ordner und wählen Sie dann die Richtlinien, die Sie konfigurieren möchten.

3 (Optional) Um Richtlinien zu aktivieren/deaktivieren, klicken Sie auf der Seite "Agent-Installation", Agent-Upgrade oder "Agent-Deinstallation" auf das Statussymbol und dann auf "Ein" oder "Aus".

4 Bringen Sie die gewünschten Konfigurationsänderungen an:

Programmname	Name des Agent-Paketprogramms, das ausgeführt wird, wenn die Richtlinie ausgelöst wird. Die Standardeinstellung ist das für die Richtlinie geeignete Programm, und normalerweise muss diese Einstellung nicht geändert werden. Vielleicht möchten Sie jedoch lieber ein neues Programm verwenden, das Sie zum Agent-Paket hinzugefügt haben. Siehe "Verwalten von Paketprogrammen" auf Seite 390.
Detaillierte Berichterstattung über Statusereignisse aktivieren	Das Senden von Paketstatusereignissen an Notification Server aktivieren. Die Einstellungen unter "Notification Server Ereigniserfassung" in der Richtlinie "Globale Symantec Management-Agent-Einstellungen" haben Vorrang gegenüber der lokalen Einstellung "Detaillierte Berichterstattung über Statusereignisse aktivieren". Ereignisse werden nur gesendet, wenn sie in der Richtlinie "Globale Symantec Management-Agent-Einstellungen" aktiviert sind. Siehe "Konfigurieren der globalen Agent-Einstellungen" auf Seite 290.
Gilt für	Gibt die Computer an, für die die Richtlinie gilt. Sie können die in Notification Server enthaltenen vordefinierten Filter verwenden oder Ihre eigenen Filter erstellen. Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.
Paket-Multicast	Deaktiviert das Herunterladen von Paketen über Multicast. Multicast verlangsamt normalerweise den Paket-Rollout. Daher ist es bei einem dringlichen Patch sinnvoll, Multicast auszuschalten. Außerdem funktioniert Multicast in bestimmten Umgebungen nicht. Es könnte beispielsweise auf Routern und Switches deaktiviert sein. Die Paket-Multicast-Einstellungen in der Richtlinie "Globale Symantec Management-Agent-Einstellungen" haben Vorrang gegenüber den lokalen Einstellungen.
Zeitplan	Gibt den Zeitplan für die Richtlinie an. Siehe "Angeben von Richtlinienzeitplänen" auf Seite 404.

Zusätzliche Zeitplanoptionen	Zusätzliche Planungsoptionen sind: ■ Einmal so bald wie möglich ausführen ■ Benutzer kann ausführen ■ Benutzer benachrichtigen, wenn die Aufgabe verfügbar ist ■ Vor Ausführung warnen

5 Klicken Sie auf "Änderungen speichern".

Infos zu Automatisierungsrichtlinien

Automatisierungsrichtlinien sind auf System- oder Administratorebene definierte Sätze von Regeln, die die Ausführung von automatisierten Aktionen regeln. Zu den automatisierten Aktionen gehören u. a. die Ausführung eines Berichts mit den aus der Richtlinie abgerufenen Parametern, Senden einer Warnmeldung an einen Administrator und Ausführung eines Befehls oder einer Aufgabe auf verwalteten Computern.

Siehe "Informationen zu Symantec Management-Plattform-Richtlinien" auf Seite 393.

Siehe "Verwalten von Automatisierungsrichtlinien" auf Seite 410.

Siehe "Schlüsselkomponenten von Automatisierungsrichtlinien" auf Seite 409.

Automatisierungsrichtlinien können auf Basis eines Zeitplan ausgeführt oder von Notification Server-Meldungen ausgelöst werden. Die Richtlinie legt fest, ob eine Aktion starten sollte, und wer oder was über die Ergebnisse benachrichtigt werden soll. Automatisierungsrichtlinien werden auf dem Notification Server-Computer ausgeführt, haben also nichts mit Agent-bezogenen Aktivitäten auf verwalteten Computer zu tun. Einige Automatisierungsrichtlinien können aber von Meldungen ausgelöst werden, die von Agent-Aktivität erzeugt wurden.

Anders als andere Arten von Notification Server-Richtlinien werden Automatisierungsrichtlinien nicht auf Ressourcenziele angewendet. Hier handelt es sich um Notification Server-Aktionen, die auf angemessenen verwalteten Computern ausgeführt werden. Einige Aktionen, wie z. B. das Senden einer E-Mail an den Administrator mit einem Bericht oder einer Datenquelle in Form einer HTML-Datei haben keine Auswirkung auf verwaltete Computer.

Viele der Lösungen, die mit Notification Server funktionieren, verfügen über Automatisierungsrichtlinien. Mit diesen Richtlinien kann Notification Server eine Vielzahl von Aktionen durchführen, wenn definierte Bedingungen auftreten. Automatisierungsrichtlinien können für einen einzelnen Prozess festgelegt werden, der auf einem Computer ausgeführt wird. Automatisierungsrichtlinien können ebenfalls für komplexe Szenarien wie zum Beispiel mehrere Prozesse auf einer Vielzahl von Computern festgelegt werden. Jede Lösung, die

Automatisierungsrichtlinien definiert, gibt ihre eigenen Kriterien für den Typ der Bedingungen an, die zu den Aktionen führen, die initiiert werden.

Inventory verwendet z. B. Daten von der CMDB und Application Metering setzt die Liste der überwachten Prozesse ein. Bei dieser Lösung gibt es allerdings gemeinsame Sätze von Aktionen, die automatisch ausgeführt werden können.

Schlüsselkomponenten von Automatisierungsrichtlinien

Siehe "Infos zu Automatisierungsrichtlinien" auf Seite 408.

Automatisierungsrichtlinien besitzen dieselben Schlüsselkomponenten.

Tabelle 25-2 Schlüsselkomponenten von Automatisierungsrichtlinien

Komponente	Beschreibung
Auslöser	Beginnt die Evaluierung einer Automatisierungsrichtlinie. Notification Server liefert die folgenden Auslöser: ■ Zeitplan Ein beliebiger Notification Server-Zeitplan, wie ein freigegebener Zeitplan oder ein angegebener benutzerdefinierter Zeitplan. Sie können keine Wartungsfenster (die auf den verwalteten Computern definiert sind) als Auslöser von Automatisierungsrichtlinien verwenden. ■ Meldung Eine interne Notification Server-Meldung. Diese werden versandt, wenn relevante Ereignisse registriert werden. Beispiele: eine Ressource wird erstellt, eine Ressource wird erkannt, eine Ressource wird gelöscht, ein neuer Computer wird erkannt oder ein Notification Server-Dienst wird gestartet.

Komponente	Beschreibung
Datenquelle	Stellt Informationen bereit, die die Automatisierungsrichtlinie nach ihrer Auslösung verwendet. Die Datenquelle ist normalerweise ein Bericht oder eine Abfrage, die eine Liste von Computern zurückgibt, zusammen mit den Informationen über den Status der einzelnen Computer und deren aktueller Einstellungen, die für die Richtlinie relevant sind. Der Bericht oder die Abfrage wird ausgeführt, wenn die Richtlinie ausgelöst wird, um sicherzustellen, dass die aktuellsten Daten extrahiert werden. Die Datenquelle definiert die von der Richtlinie angezielten verwalteten Computer und die auf diesen ausgeführten Aktionen. Eine Automatisierungsrichtlinie kann auch Parameter aus der Datenquelle extrahieren und sie dann als Eingabeparameter für Aufgaben oder Jobs verwenden. Notification Server stellt folgende Datenquellen bereit: ■ Bericht ■ Rohe SQL-Abfrage Wenn Sie diese Option auswählen, benötigen Sie das Recht "Edit SQL Directly", um in der Lage zu sein, die Datenquelleabfrage zu bearbeiten und die Abfrageergebnisse anzuzeigen. Siehe "Systemrechte" auf Seite 516. ■ Ressourcenabfrage ■ Meldung ■ Keine Lösungen können zusätzliche Datenquellen hinzufügen.
Auswertungsregel	Evaluiert die Daten, die in der Datenquelle enthalten sind, und stellt fest, ob eine Aktion ausgeführt werden soll oder nicht. Notification Server stellt folgende Evaluierungsregeln bereit: ■ Für gefüllte Datensätze ausführen ■ Für jeden Datensatz ausführen ■ Nachrichtenverarbeitung ■ Immer ausführen
Aktion	Gibt die Aufgabe oder den Job an, die/den die Richtlinie ausführt. Es handelt sich dabei um Standard-Agent- oder serverseitige Aufgaben. Die Aktion kann Eingabeparameter einschließen, die von der Datenquelle weitergegeben werden.

Verwalten von Automatisierungsrichtlinien

Sie können die Automatisierungsrichtlinien konfigurieren und verwalten, die auf dem Notification Server verfügbar sind. Sie können neue Richtlinien erstellen, vorhandene Richtlinien bearbeiten, eine Richtlinie bei Bedarf aktivieren oder

deaktivieren, die gewünschte Sicherheit für eine Richtlinie einstellen und eine Richtlinie löschen, wenn diese nicht mehr benötigt wird.

Siehe "Infos zu Automatisierungsrichtlinien" auf Seite 408.

Sie verwalten Sie Automatisierungsrichtlinien

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Automatisierungsrichtlinien".
2. Wählen Sie auf der Seite "Automatisierungsrichtlinien" die entsprechende Registerkarte aus:

Zeitpläne	Automatisierungsrichtlinien verwalten, die unter einem definierten Zeitplan ausgeführt werden.
Systemmeldungen	Automatisierungsrichtlinien verwalten, die ausgeführt werden, wenn eine bestimmte Systemmeldung eingeht.

3 Führen Sie einen der folgenden Schritte aus:

Eine Richtlinie erstellen oder ändern	Siehe "Erstellen und Ändern von geplanten Automatisierungsrichtlinien" auf Seite 414. Siehe "Erstellen und Ändern von meldungsbasierten Automatisierungsrichtlinien" auf Seite 416.
Eine Richtlinie aktivieren oder deaktivieren	Wählen Sie im linken Teilfenster die Automatisierungsrichtlinie, die Sie aktivieren bzw. deaktivieren möchten, und klicken Sie dann auf "Einschalten" bzw. "Ausschalten".
Eine Richtlinie löschen	Wählen Sie im linken Teilfenster die zu löschende Automatisierungsrichtlinie aus und klicken Sie dann auf "Löschen". Sie können alle Automatisierungsrichtlinien löschen, die Sie erstellt haben. Sie können aber nicht die Standard-Automatisierungsrichtlinien löschen, die mit Notification Server bereitgestellt werden.
Sicherheit für eine Richtlinie festlegen	Im linken Teilfenster wählen Sie die Automatisierungsrichtlinie, deren Sicherheit Sie festlegen möchten, und klicken Sie dann auf "Aktionen" > "Sicherheit". Legen Sie im Sicherheitsrollenmanager die entsprechenden Sicherheitseinstellungen fest.
Weitere Aktionen für eine Richtlinie ausführen	Wählen Sie im linken Feld die Automatisierungsrichtlinie, für die Sie eine Aktion ausführen möchten, klicken Sie auf Aktionen und dann auf die gewünschte Option. Die verfügbaren Aktionen sind mit denen im Kontextmenü identisch.
Eine Richtlinie testen	Wählen Sie im linken Bereich die zu testende Automatisierungsrichtlinie aus und klicken Sie dann im rechten Bereich auf Automatisierungsrichtlinie testen. Sie können den Automatisierungsrichtlinientest verwenden, um zu testen, ob alle Richtlinienkomponenten konsistent sind und die Eingabeparameter ordnungsgemäß zugeordnet wurden. Der Test führt die Richtlinie aus und die Ergebnisse der Aktion werden im Job-/Aufgabe-Protokoll angezeigt.

Erstellen und Ändern von geplanten Automatisierungsrichtlinien

Automatisierungsrichtlinien können einen beliebigen Notification Server-Zeitplan verwenden, wie z. B. einen gemeinsam genutzten Zeitplan oder einen festgelegten benutzerdefinierten Zeitplan. Wartungsfenster (die auf verwalteten Computern definiert sind) können nicht zur Planung von Automatisierungsrichtlinien verwendet werden. Wenn eine Automatisierungsrichtlinie ausgelöst wird, werden die entsprechenden Aktionen sofort ausgeführt. Sie können eine Automatisierungsrichtlinie nicht zur Ausführung zu einem späteren Zeitpunkt planen, nachdem diese ausgelöst wurde.

Siehe "Infos zu Automatisierungsrichtlinien" auf Seite 408.

Siehe "Verwalten von Automatisierungsrichtlinien" auf Seite 410.

Hinweis: In diesem Themenbereich werden die mit Notification Server bereitgestellten Standardoptionen abgedeckt. Lösungen können über erweiterte oder neue Optionen verfügen. Weitere Informationen finden Sie in der Dokumentation zur jeweiligen Lösung.

So erstellen oder ändern Sie ein geplante Automatisierungsrichtlinie

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Automatisierungsrichtlinien".
2. Auf der Seite "Automatisierungsrichtlinien" auf der Registerkarte "Zeitpläne" haben Sie folgende Möglichkeiten:

So erstellen Sie eine neue Richtlinie	1 Klicken Sie auf "Neue Richtlinie". 2 Geben Sie im Dialogfeld "Name der neuen Automatisierungsrichtlinie" einen Namen ein und klicken Sie auf "OK".
So ändern Sie eine bestehende Richtlinie	Wählen Sie im linken Teilfenster die gewünschte Richtlinie aus.

3. (Optional) Bearbeiten Sie im rechten Bereich den Richtliniennamen und die Beschreibung, indem Sie auf die entsprechenden Felder klicken.

4 Wählen Sie in der Dropdown-Liste Zeitplan den gewünschten Zeitplan aus.

Am/Um	Geben Sie Datum, Uhrzeit und Wiederholungshäufigkeit in die jeweiligen Felder ein.
Gemeinsam genutzter Zeitplan	Wählen Sie in der Dropdown-Liste "Gemeinsam genutzten Zeitplan auswählen" den gewünschten Zeitplan aus. Siehe "Verwalten gemeinsam genutzter Zeitpläne" auf Seite 128.

5 Geben Sie im Bereich "Details" unter "Datenquelle" die gewünschte Datenquelle an.

Siehe "Angeben der Datenquelle für Automatisierungsrichtlinien" auf Seite 419.

6 Wählen Sie unter "Bedingungen" in der Dropdown-Liste "Auswertungsregel" die gewünschte Auswertungsregel aus:

Für gefüllte Datensätze ausführen	Verarbeitet die Datenquellentabelle als einzelne Einheit. Wenn die Richtlinie ausgelöst wird, wird die Aktion nur ausgeführt, wenn die Tabelle mindestens eine Zeile enthält; die Richtlinie wird nur ein Mal ausgeführt. Sie müssen diese Option verwenden, wenn die Datenquelle Informationen in einer HTML-Datei und nicht in einer Tabelle enthält. Mit dieser Option können Sie auf alles in einer einzelnen Spalte abzielen, wie z. B. einer Liste von GUIDs. Sie können dynamische Parameter zur Unterscheidung von Zielcomputern festlegen. In diesem Fall müssen Sie "Ausführen" für jede Datensatzoption festlegen.
Für jeden Datensatz ausführen	Wertet die Datenquelltabelle Zeile für Zeile aus. Dieses Vorgehen ermöglicht es Ihnen, Felder pro Zeile als dynamische Parameter für die angegebenen Aktionen einzusetzen. Diese Aktion wird nur ein Mal pro Zeile ausgeführt.
Immer ausführen	Führt die festgelegten Aktionen ohne Verwendung einer Datenquelle aus. Diese Option ist nur dann verfügbar, wenn keine Datenquelle angegeben wird.

7 Geben Sie unter "Aktionen" die gewünschte Aufgabe bzw. den Job an und legen Sie erforderliche Eingabeparameter fest.

Siehe "Festlegen der Aktion für Automatisierungsrichtlinien" auf Seite 421.

8 Klicken Sie auf "Übernehmen", um die Richtlinieneinstellungen zu speichern.

9 (Optional) Um zu gewährleisten, dass alle Richtlinienkomponenten konsistent und die Eingabeparameter ordnungsgemäß zugeordnet sind, klicken Sie auf "Automatisierungsrichtlinie testen".

Dieser Test ist lediglich eine interne Überprüfung und hat keine Auswirkung auf Ressourcen.

Erstellen und Ändern von meldungsbasierten Automatisierungsrichtlinien

Automatisierungsrichtlinien können eine interne Notification Server-Meldung als Auslöser verwenden. Die für diesen Zweck vorhandenen Meldungen sind vordefiniert. Diese Meldungen beziehen sich auf Notification Server-Ereignisse wie die Erkennung, Erstellung oder Löschung von Ressourcen, die Erkennung neuer Computer oder den Start von Notification Server-Diensten. Lösungen stellen u. U. zusätzliche lösungsspezifische Meldungen bereit. Wenn eine Automatisierungsrichtlinie ausgelöst wird, werden die entsprechenden Aktionen sofort ausgeführt. Nachdem eine Automatisierungsrichtlinie ausgelöst wurde, können Sie sie nicht zur Ausführung zu einem späteren Zeitpunkt konfigurieren.

Siehe "Infos zu Automatisierungsrichtlinien" auf Seite 408.

Siehe "Verwalten von Automatisierungsrichtlinien" auf Seite 410.

Hinweis: Dieses Thema enthält die Standardoptionen, die in der Symantec Management-Plattform enthalten sind. Lösungen können über erweiterte oder neue Optionen verfügen. Weitere Informationen finden Sie in der Dokumentation zur jeweiligen Lösung.

So erstellen oder ändern Sie eine meldungsabhängige Automatisierungsrichtlinie

1 Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Automatisierungsrichtlinien".

2 Auf der Seite "Automatisierungsrichtlinien" auf der Registerkarte "Systemmeldungen" haben Sie folgende Möglichkeiten:

So erstellen Sie eine neue Richtlinie	1 Klicken Sie auf "Neue Richtlinie". 2 Geben Sie im Dialogfeld "Name der neuen Automatisierungsrichtlinie" einen Namen ein und klicken Sie auf "OK".
So ändern Sie eine bestehende Richtlinie	Wählen Sie im linken Teilfenster die gewünschte Richtlinie aus.

3 (Optional) Bearbeiten Sie im rechten Bereich den Richtliniennamen und die Beschreibung, indem Sie auf die entsprechenden Felder klicken.

4 Wählen Sie in der Dropdown-Liste "NS-Nachricht" die gewünschte Meldung aus.

5 Geben Sie im Bereich "Details" unter "Datenquelle" die gewünschte Datenquelle an.

Siehe "Angeben der Datenquelle für Automatisierungsrichtlinien" auf Seite 419.

6 Wählen Sie unter "Bedingungen" in der Dropdown-Liste "Auswertungsregel" die gewünschte Auswertungsregel aus:

Für gefüllte Datensätze ausführen	Verarbeitet die Datenquellentabelle als einzelne Einheit. Wenn die Richtlinie ausgelöst wird, wird die Aktion nur ausgeführt, wenn die Tabelle mindestens eine Zeile enthält; die Richtlinie wird nur ein Mal ausgeführt. Sie müssen diese Option verwenden, wenn die Datenquelle Informationen in einer HTML-Datei und nicht in einer Tabelle enthält. Mit dieser Option können Sie auf alles in einer einzelnen Spalte abzielen, wie z. B. einer Liste von GUIDs. Sie können dynamische Parameter zur Unterscheidung von Zielcomputern festlegen. In diesem Fall müssen Sie "Ausführen" für jede Datensatzoption festlegen.
Für jeden Datensatz ausführen	Wertet die Datenquelltabelle Zeile für Zeile aus. Dieses Vorgehen ermöglicht es Ihnen, Felder pro Zeile als dynamische Parameter für die angegebenen Aktionen einzusetzen. Diese Aktion wird nur ein Mal pro Zeile ausgeführt.
Nachrichtenverarbeitung	Evaluiert den Text der Meldung der Datenquelle und verwendet die entsprechenden Parameter in den angegebenen Aktionen. Diese Option ist nur verfügbar, wenn eine Meldungsdatenquelle verwendet wird.
Immer ausführen	Führt die festgelegten Aktionen ohne Verwendung einer Datenquelle aus. Diese Option ist nur dann verfügbar, wenn keine Datenquelle angegeben wird.

7 Geben Sie unter "Aktionen" die gewünschte Aufgabe bzw. den Job an und legen Sie erforderliche Eingabeparameter fest.

Siehe "Festlegen der Aktion für Automatisierungsrichtlinien" auf Seite 421.

8 Klicken Sie auf "Änderungen speichern", um die Richtlinieneinstellungen zu speichern.

9 (Optional) Um zu gewährleisten, dass alle Richtlinienkomponenten konsistent und die Eingabeparameter ordnungsgemäß zugeordnet sind, klicken Sie auf "Automatisierungsrichtlinie testen".

Dieser Test ist lediglich eine interne Überprüfung und hat keine Auswirkung auf Ressourcen.

Angeben der Datenquelle für Automatisierungsrichtlinien

Die Datenquelle der Automatisierungsrichtlinie bestimmt, welche Computer berücksichtigt und welche Aktionen auf ihnen ausgeführt werden sollen. Eine Automatisierungsrichtlinie kann Parameter aus der Datenquelle extrahieren und sie dann als Eingabeparameter für Aufgaben oder Jobs verwenden.

Siehe "Erstellen und Ändern von geplanten Automatisierungsrichtlinien" auf Seite 414.

Siehe "Erstellen und Ändern von meldungsbasierten Automatisierungsrichtlinien" auf Seite 416.

Sie können externe Datenquellen wie Berichte und Meldungen verwenden, oder Sie können eine Abfrage zur Extrahierung vom CMDB verwenden. Eine externe Datenquelle wie ein Bericht kann von einer beliebigen Anzahl Automatisierungsrichtlinien verwendet werden. Sie müssen sorgfältig sein, wenn Sie Berichte verwenden, weil diese später geändert und die Parameter, von denen einige Aktionen abhängen, geändert oder entfernt werden könnten. Falls eine Aktion einen erforderlichen Parameter nicht von einem Datenquellenbericht her festlegen kann, verwendet sie den Standardwert, der in der Automatisierungsrichtlinie eingestellt ist.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

SQL- und Ressourcenabfragen sind in der Definition der Automatisierungsrichtlinie eingebettet. Sie können Abfragen nicht zwischen Automatisierungsrichtlinien teilen, und Sie können nicht direkt auf die Abfragen (die auch als Datenquellen bekannt sind) zugreifen, die Komponenten von Berichten sind. Wenn Sie eine Berichtabfrage verwenden möchten, können Sie den SQL-Code aus dem Bericht kopieren und in die Automatisierungsrichtlinie einfügen.

Eine Automatisierungsrichtlinie, die kein Ziel für ihre Aktion definiert, erfordert keine Datenquelle. Beispiel: Eine Richtlinie, die eine Meldung an den Administrator sendet, oder eine Aufgabe auf dem Notification Server-Computer ausführt.

So geben Sie die Datenquelle der Automatisierungsrichtlinie an

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Automatisierungsrichtlinien".
2. Wählen Sie auf der Seite "Automatisierungsrichtlinien" auf der Registerkarte "Systemmeldungen" entweder eine vorhandene Automatisierungsrichtlinie aus oder erstellen Sie eine neue.
3. Wählen Sie im rechten Teilfenster unter "Details" unter "Datenquelle" in der Dropdown-Liste "Datenquelle" die entsprechende Option aus:

Bericht	Verwenden Sie die Ergebnisse eines Berichts. 1 Klicken Sie im Feld "Bericht" auf "Berichtname". 2 Wählen Sie im Fenster "Bericht auswählen" den entsprechenden Bericht aus und klicken Sie dann auf "OK".
Rohe SQL-Abfrage	Verwenden Sie die Ergebnisse einer SQL-Abfrage. 1 Klicken Sie auf "Abfrage bearbeiten". 2 Geben Sie im Fenster "Datenquelle" die SQL-Abfrage an, die Sie verwenden möchten, und klicken Sie dann auf "OK". Siehe "Definieren einer SQL-Abfrage für einen Filter" auf Seite 377. Wenn Sie eine Abfrage von einem vorhandenen Filter oder Bericht wieder verwenden möchten, können Sie den Inhalt der Registerkarte "Gelöste Abfrage" vom entsprechenden Filter oder der Berichtabfrage kopieren. Sie können sie dann auf der Registerkarte "Abfrageauflösung" im Fenster "Datenquelle" einfügen. Nun können Sie den SQL-Code nach Bedarf ändern. Beachten Sie, dass auf der Registerkarte "Abfrageauflösung" alle Parameter der Abfrage durch die angegebenen Testwerte ersetzt wurden.
Ressourcenabfrage	Verwenden Sie die Ergebnisse einer Ressourcenabfrage. 1 Klicken Sie auf "Abfrage bearbeiten". 2 Geben Sie im Fenster "Datenquelle" die Ressourcenabfrage an, die Sie verwenden möchten, und klicken Sie dann auf "OK". Siehe "Definieren einer Ressourcenabfrage für einen Filter" auf Seite 374.
Meldung	Verwenden Sie die Informationen in der Meldung, die die Richtlinie ausgelöst hat.

Keiner	Es ist keine Datenquelle erforderlich. Die Automatisierungsrichtlinie braucht kein Ziel für ihre Aktion zu definieren.

Festlegen der Aktion für Automatisierungsrichtlinien

Bei Aktionen für Automatisierungsrichtlinien handelt es sich um Jobs und Aufgaben. Symantec Management-Plattform liefert einen Satz von Aufgaben, die Sie verwenden können, und durch Lösungen können weitere hinzugefügt werden. Sie können Ihre eigenen Aufgaben erstellen und die Optionen Ihren Anforderungen entsprechend erweitern. Wenn Ihre Symantec Management-Plattform Teil einer Hierarchie ist, können weitere Aufgaben und Jobs in der übergeordneten Symantec Management-Plattform abwärts repliziert werden.

Siehe "Erstellen und Ändern von geplanten Automatisierungsrichtlinien" auf Seite 414.

Siehe "Erstellen und Ändern von meldungsbasierten Automatisierungsrichtlinien" auf Seite 416.

Eine Automatisierungsrichtlinie enthält möglicherweise nur eine Aktion, bei der es sich unter Umständen um eine Aufgabe oder einen Job handeln kann, der auf alle Zielcomputer der Richtlinie angewendet wird. Wenn Sie mehrere Aufgaben einschließen möchten, müssen Sie sie in einen geeigneten Job einbinden. Außerdem müssen Sie mehrere Automatisierungsrichtlinien mit den entsprechenden Auslösern, Datenquellen und Aktionen erstellen.

Warnung: Eine beliebige Anzahl von Automatisierungsrichtlinien kann einen Job oder eine Aufgabe gemeinsam nutzen. Wenn Sie eine Aufgabe ändern, die in einer Automatisierungsrichtlinie verwendet werden soll, können sich Ihre Änderungen auf viele anderen Richtlinien auswirken. Sie ziehen es möglicherweise vor, die relevante Aufgabe zu duplizieren und die geänderte Duplizierung in der Richtlinie zu verwenden.

Aufgaben können sowohl statische als auch dynamische Eingabeparameter enthalten. Dynamische Parameter werden mit den Werten festgelegt, die aus der Datenquelle extrahiert werden, sobald die Richtlinie ausgelöst wird. Statische Parameter verfügen über innerhalb der Aufgabe festgelegte Werte. Es sind bei jedem Ausführen der Aufgabe die gleichen Werte.

Fehleraktionen oder Rückgabecodes können in einer Automatisierungsrichtlinie nicht festgelegt werden. Somit müssen Sie sie bei Bedarf in der Aufgabe konfigurieren.

So legen Sie Aktionen für Automatisierungsrichtlinien fest

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Automatisierungsrichtlinien".
2. Wählen Sie auf der Seite "Automatisierungsrichtlinien" auf der Registerkarte "Systemmeldungen" entweder eine vorhandene Automatisierungsrichtlinie aus oder erstellen Sie eine neue.
3. Klicken Sie im rechten Teilfenster unter "Aktionen" im Feld "Job/Aufgabe ausführen" auf "Job oder Aufgabe auswählen".
4. Wählen Sie im Dialogfeld "Aufgabe auswählen" im linken Teilfenster den entsprechenden Job oder die entsprechende Aufgabe aus und klicken Sie anschließend auf "OK".

   Siehe "Auswählen von Aufträgen oder Aufgaben für die Automatisierungsrichtlinie" auf Seite 423.
5. (Optional) Klicken Sie auf "Eingabeparameter bearbeiten", und geben Sie anschließend im Dialogfeld "Job/Aufgabe bearbeiten - Eingabeparameter" Folgendes für jeden Aktionsparameter an:

Datenquelle	Das Feld "Datenquelle", das den Parameter liefert. Wählen Sie die entsprechende Option aus der Dropdown-Liste aus: ■ Ergebnisse als HTML-Datei ■ Ergebnisse als CSV-Datei ■ Ergebnisse als Textdatei ■ Zeilenanzahl ■ Benutzerdefiniert
Benutzerdefinierter Wert	Der Wert, der verwendet wird, wenn für die Datenquelle "Benutzerdefiniert" festgelegt wird. Dieser Wert ist die verwendete Standardeinstellung, wenn das Feld "Angegebene Datenquelle" nicht verfügbar ist.

   Dieses Feld wird nicht angezeigt, wenn keine Eingabeparameter erforderlich sind.
6. (Optional) Klicken Sie auf "OK", um das Fenster "Job/Aufgabe bearbeiten - Eingabeparameter" zu schließen.
7. Klicken Sie auf "Änderungen speichern".

Auswählen von Aufträgen oder Aufgaben für die Automatisierungsrichtlinie

Im Fenster "Aufgabe auswählen" können Sie den Auftrag oder die Aufgabe auswählen, der/die durchgeführt werden soll, wenn die Automatisierungsrichtlinie ausgelöst wird.

Siehe "Festlegen der Aktion für Automatisierungsrichtlinien" auf Seite 421.

Im linken Teilfenster wird die Ordnerstruktur "Task Management" angezeigt. Es enthält alle Aufgaben, die für die Verwendung in Automatisierungsrichtlinien zur Verfügung stehen. Im rechten Teilfenster wird die Seite "Aufgabenkonfiguration" für die ausgewählte Aufgabe angezeigt. Hier können Sie alle notwendigen Änderungen vornehmen.

So wählen Sie einen Auftrag oder eine Aufgabe für die Automatisierungsrichtlinie aus

1. Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Automatisierungsrichtlinien".
2. Wählen Sie auf der Seite "Automatisierungsrichtlinien" auf der Registerkarte "Systemmeldungen" entweder eine vorhandene Automatisierungsrichtlinie aus oder erstellen Sie eine neue.
3. Klicken Sie im rechten Teilfenster unter "Aktionen" im Feld "Job/Aufgabe ausführen" auf "Job oder Aufgabe auswählen".
4. Wählen Sie im Dialogfeld "Aufgabe auswählen" im linken Teilfenster den entsprechenden Job oder die entsprechende Aufgabe aus und nehmen Sie dann im rechten Teilfenster alle notwendigen Konfigurationsänderungen am Job oder an der Aufgabe vor.
5. Klicken Sie auf "OK".

Erstellen und Ändern von Automatisierungsrichtlinien-Aufgaben

Ein Satz Automatisierungsrichtlinieaufgaben ist in der Symantec Management-Plattform enthalten. Sie können sie in Ihren Automatisierungsrichtlinien und als Vorlage zur Erstellung Ihrer eigenen benutzerdefinierten Aufgaben und Aufträge verwenden.

Siehe "Festlegen der Aktion für Automatisierungsrichtlinien" auf Seite 421.

Mit den Aufgaben können Sie folgende Aktionen ausführen:

Einer Organisationsgruppe zuweisen	Hier können Sie Ressourcen einer Organisationsgruppe zuweisen.
Bericht per E-Mail senden	Hier können Sie einen angegebenen Bericht als E-Mail-Anhang senden. Sie sollten diese Aufgabe als Teil eines Auftrags verwenden, der auch eine Aufgabe zum Ausführen eines Berichts enthält, um den entsprechenden Bericht zu erstellen.
E-Mail senden	Hier können Sie eine E-Mail mit Informationen an die angegebenen Benutzern senden. Die E-Mail kann Status-, Produktlizenz- oder andere Informationen enthalten.
Bericht ausführen	Sie sollten diese Aufgabe als Teil eines Auftrags verwenden, der auch eine Aufgabe zum Senden eines Berichts per E-Mail an geeignete Benutzer oder den Notification Server-Administrator enthält.

So erstellen oder ändern Sie eine Automatisierungsrichtlinienaufgabe

1. Klicken Sie in Symantec Management Console im Menü "Verwalten" auf "Jobs und Aufgaben".
2. Erweitern Sie im linken Teilfenster den Ordner "Jobs und Aufgaben" > "Systemjobs und -aufgaben" > "Notification Server" > "Automatisierungsrichtlinien-Aufgaben" und wählen Sie eine der folgenden Optionen aus:

So erstellen Sie einen neuen Job oder eine Aufgabe	1 Klicken Sie mit der rechten Maustaste auf den Ordner "Automatisierungsrichtlinien-Aufgaben", dann auf "Neu" und schließlich auf die gewünschte Option. 2 Wählen Sie im Dialogfeld "Neue Aufgabe erstellen" im linken Teilfenster die Aufgabe aus. 3 Geben Sie im rechten Teilfenster die Optionen an und klicken Sie dann auf "OK".
So erstellen Sie einen neuen Job oder eine neue Aufgabe unter Verwendung eines vorhandenen Jobs bzw. einer Aufgabe als Vorlage	Klicken Sie mit der rechten Maustaste auf den Job bzw. die Aufgabe, und klicken Sie dann auf "Duplizieren".
So ändern Sie einen vorhandenen Job bzw. eine Aufgabe	Klicken Sie auf den Job bzw. die Aufgabe.

3 Machen Sie im rechten Teilfenster die entsprechenden Angaben.

4 Klicken Sie auf "Änderungen speichern".

Kapitel 26

Verwenden von Aufgaben und Aufträgen

In diesem Kapitel werden folgende Themen behandelt:

- Informationen zu Task Management
- Task Management-Komponenten
- Wie Task Server die Tickle-Funktion verwendet
- Verwendung von Aufgaben, Jobs und Richtlinien
- Informationen zu ausgeführten Aufgaben in der Hierarchie
- Sequenzieren von Aufgaben
- Anzeigen und Bearbeiten von Berechtigungen für einen Aufgabentyp
- Erstellen von Aufgaben für die Eingabe oder Ausgabe von Aufgabeneigenschaften
- Bereinigen von Aufgabendaten
- Bereinigen von Aufgabenversionsdaten
- Ändern der Client Task Agent-Einstellungen
- Zugriff auf das Job- und Aufgabenportal

Informationen zu Task Management

Das Task Management stellt die Aufgabensequenzierung und -automatisierung für Symantec-Lösungen zur Verfügung. Mithilfe der Aufgabensequenzierung können Sie komplexe Verwaltungsvorgänge in einem einzelnen Job durchführen. Aufgaben

können in einem Job sequenziell angeordnet werden, wodurch Sie höhere Flexibilität bei Ihrer Arbeit haben. Die Funktionsweise ähnelt der der Job-Engine der Symantec Deployment Solution. Jedoch ist Task Management in die Symantec Management-Plattform integriert. Dadurch kann der übrige Symantec-Lösungskatalog Nutzen aus ihren leistungsfähigen Funktionen ziehen.

Siehe "Sequenzieren von Aufgaben" auf Seite 436.

Sie können Aufgaben basierend auf Ereignissen im System oder Änderungen in der Datenbank automatisch ausführen. Sie können Aufgaben auch automatisch ausführen, damit Computer weiterhin mit den Richtlinien konform sind.

Task Server ähneln Package Servern dahingehend, dass sie entwickelt wurden, um auf einem separaten Server eingerichtet zu werden, und sehr kompakt sind. Task Server und Package Server sind Site Services und werden auf einem Site Server installiert. Computer kann einem bestimmten Site Server entweder nach Computername oder Subnetz zugewiesen werden.

Siehe "Info zu Site Services" auf Seite 133.

Sie können dieses "Jobs und Aufgaben"-Portal beim Erstellen, Ausführen oder Planen von Jobs und Aufgaben verwenden. Die Aufgabekomponenten begleiten diese Aufträge und Aufgaben ohne Probleme.

Siehe "Task Management-Komponenten" auf Seite 428.

Task Management umfasst die folgenden Funktionen:

- Führt mehrere Aufgaben in einer definierten Reihenfolge aus, die als Job bezeichnet wird.
  Siehe "Erstellen eines Jobs" auf Seite 439.
- Damit kann den Benutzern eine Logik zur Verarbeitung von Aufgabenfehlern oder anderen Rückgabecodes zur Verfügung gestellt werden.
- Enthält leistungsfähige Kommandozeilen- und VBscript-Funktionen.
- Stellt vordefinierte Energieverwaltungsaufgaben zur Verfügung.
- Führt clientseitige und serverseitige Aufgaben aus.
  Siehe "Bereitstellen eines Task Server" auf Seite 437.
- Stellt schnelle Funktionen für laufende Jobs zur Verfügung, wie beispielsweise die Optionen "Jetzt ausführen" und Statusrückmeldungen annähernd in Echtzeit.
  Siehe "Ausführen eines Jobs oder einer Aufgabe" auf Seite 442.
  Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.
  Siehe "Anzeigen des Aufgabenstatus auf dem Symantec Management-Agent" auf Seite 445.

- Sie können Aufgaben in mehreren Aufträgen erneut verwenden oder Aufgaben duplizieren und ändern.

Task Management-Komponenten

Task Management-Arbeiten mittels Nutzung verschiedener Komponenten. Diese Komponenten stimmen die Zuweisung und die Leistung von Aufgaben und Aufträgen auf den verbundenen Clientcomputern ab.

Siehe "Informationen zu Task Management " auf Seite 426.

Tabelle 26-1 Task Management-Komponenten

Komponente	Beschreibung
Task Server	Diese Komponente verteilt Aufträge und Aufgaben auf dem Netzwerk, und sie kann auf dem Notification Server oder auf einem Remote-Computer ausgeführt werden. Der Task Server hat die Fähigkeit, Tickles an die registrierten Clientcomputer zu senden. Diese Tickle-Funktion unterscheidet sich vom Tickle Server auf dem Notification Server-Computer. Der Task Server sendet die Statusangaben zum Data Loader. Er sendet auch die Tickles, den Auftrag und die Aufgabeninformationen an den Client Task Agent.
Tickle-Server	Der Tickle-Server benachrichtigt den Task Server, wann und wo Aufgaben auf den verbundenen Client-Computern ausgeführt werden sollen. Der Tickle-Server sendet dann Tickles an diese verbundenen Client-Computer und sendet dann über HTTP(S) XML-Dateien mit den Job- oder Aufgabeninformationen. Außerdem erfasst der Tickle-Server Statusinformationen und leitet diese über HTTP(S) an die Konfigurationsmanagement-Datenbank (CMDB) weiter. Diese Komponente wird ausschließlich auf dem Notification Server-Computer ausgeführt. Sie sendet ein IP-Tickle-Paket an Task Server, wenn einer der Clients einen Auftrag oder eine Aufgabe ausführen soll. Siehe "Wie Task Server die Tickle-Funktion verwendet" auf Seite 429.

Komponente	Beschreibung
Data Loader	Diese Komponente erhält Statusinformationen von Task Servern und speichert sie im Arbeitsspeicher, bis sie an die CMDB gesendet werden können. Der Data Loader verbessert die Skalierbarkeit, indem Statusinformationen für mehrere hundert Clients zur selben Zeit empfangen werden können, ohne den SQL Server zu überlasten. Diese Komponente wird auch auf jedem Remote-Task Server ausgeführt und stellt Daten in die Warteschlange, bis sie an den Notification Server gesendet werden können.
Client Task Agent	Dieser Agent läuft auf Clientcomputern und führt die folgenden Aktionen aus: ■ Akzeptiert Tickles von einem Task Server. ■ Empfängt die Auftrags- und die Aufgabeninformationen. ■ Gibt die Informationen an eine Behandlungsroutine weiter. ■ Sendet die Statusinformationen an den Task Server zurück. Dieser Agent wird automatisch mit dem Symantec Management-Agent installiert. **Hinweis:** Wenn Sie den Symantec Management-Agent auf einem Computer installieren, gibt es eine Verzögerung, bevor der Client Task Agent auf dem Notification Server registriert wird. Alle Aufgaben, die während dieser Zeit (gewöhnlich ca. 10 Minuten) diesen Computer als Ziel haben, werden in die Warteschlange gestellt, bis der Client Task Agent registriert wurde. Nachdem der Client Task Agent registriert wurde, werden die Aufgaben sofort ausgeführt.

Wie Task Server die Tickle-Funktion verwendet

Der Tickle-Server ist eine Komponente von Task Management. Diese Komponente wird nur auf dem Notification Server ausgeführt und ist dafür verantwortlich, Task Server von bevorstehenden Aufgaben für ihre Clientcomputer zu unterrichten. Task Server haben auch die systemeigene Fähigkeit, Tickles an ihre registrierten Clientcomputer zu senden. Diese Tickle-Funktion unterscheidet sich vom Tickle Server auf dem Notification Server-Computer.

Siehe "Task Management-Komponenten" auf Seite 428.

Der Tickle Server sendet ein IP-Tickle-Paket an Task-Server, wenn einer seiner registrierten Clientcomputer einen Auftrag oder eine Aufgabe auszuführen hat. Nach Empfang des Tickle-Pakets fordert der Task Server sofort die Aufgaben- oder

Auftragsinformationen vom Notification Server für seine registrierten Clientcomputer an. Er sendet auch Tickles an seine Clientcomputer. Wenn der Client Task Agent das Tickle-Paket empfängt, fordert er die Auftrags- oder Aufgabeninformationen von seinem registrierten Task Server an. Die Aufgabe wird erst ausgeführt, nachdem der Client Task Agent die Aufgabeninformationen erhält. Statusereignisse für vollständige Aufgaben werden nach Beendung an den registrierten Task Server zurückgesandt.

Wenn die Tickle-Pakete blockiert sind oder ihr Ziel sonst nicht erreichen können, richtet sich der Client Task Agent automatisch an seinen registrierten Task Server, um neue Jobinformationen anzufordern. Er führt diese Prüfung alle 5 Minuten aus. Dieses Intervall zur Aufgabenanforderung kann in der Symantec Management Console konfiguriert werden. Task Server-Aufgaben- und Auftragsinformationen werden nicht durch die Konfigurationsrichtlinie des Symantec Management-Agent empfangen. Der Client Task Agent empfängt sie direkt von seinem registrierten Task Server. Wenn Sie den Symantec Management-Agent zur Aktualisierung seiner Konfigurationsrichtinie zwingen, wird der Empfang von Informationen über bevorstehende Aufgaben durch den Client Task Agent nicht erzwungen.

Siehe "Ändern der Client Task Agent-Einstellungen" auf Seite 451.

Standardmäßig verwendet der Tickle Server Port 50123 für Task Server, und Task Server verwenden Port 50124, um Client Task Agents Tickles zu senden.

Siehe "Informationen zu Task Management " auf Seite 426.

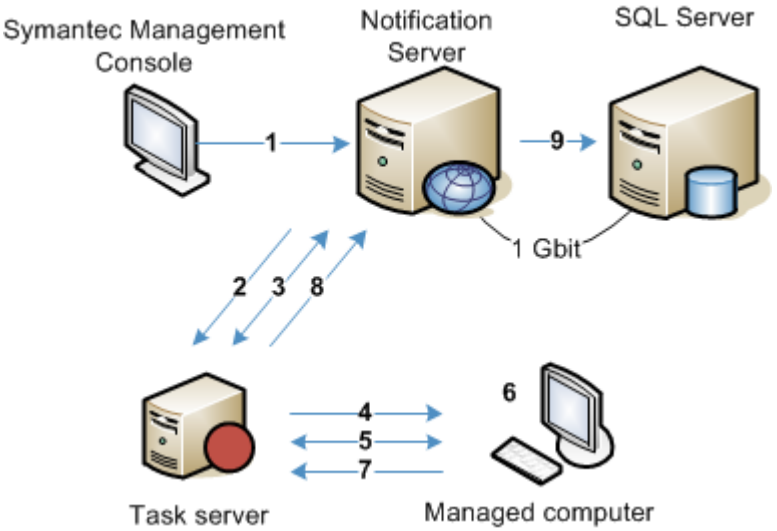
Im folgenden Beispiel wird angenommen, dass der Client Task Agent für ComputerA mit RemoteTaskServer1 registriert ist.

Tabelle 26-2 Reihenfolge, in der der Task Server Tickle verarbeitet

Reihenfolge	Beschreibung
Eins	Ein Notification Server-Administrator weist eine Aufgabe zu, die sofort auf ComputerA ausgeführt werden soll.
Zwei	Der Tickle Server auf dem Notification Server-Computer sendet ein Tickle-Paket, um RemoteTaskServer1 von der bevorstehenden Aufgabe zu unterrichten.
Drei	RemoteTaskServer1 prüft, ob der Zielclient beliebige Aufgaben erhalten darf. Ist der Modus "Legacy-Agent-Kommunikation" deaktiviert und ist das Ziel ein Legacy-Agent, schlägt die Aufgabe sofort fehl. Sie schlägt auch fehl, wenn der Agent aktualisiert wird, sich aber im Zustand "Nicht zulässig" befindet. Siehe "Info zu Agent-Registrierung" auf Seite 247.

Reihenfolge	Beschreibung
Vier	RemoteTaskServer1 empfängt das Tickle-Paket und fordert sofort die Auftragsinformationen vom Notification Server an.
Fünf	RemoteTaskServer1 sendet Tickles an ComputerA, um diesen von der bevorstehenden Aufgabe zu unterrichten.
Sechs	ComputerA empfängt das Tickle-Paket und fordert sofort die Auftragsinformationen von seinem registrierten Task Server (RemoteTaskServer1) an.
Sieben	ComputerA empfängt die Auftragsinformationen und führt die Aufgabe aus.
Acht	Nach Abschluss der Aufgabe sendet ComputerA ein Statusereignis zurück an RemoteTaskServer1.
Neun	RemoteTaskServer1 speichert das Statusereignis zwischen und versucht sofort, es an den Notification Server weiterzuleiten.
Zehn	Notification Server empfängt das Statusereignis vom RemoteTaskServer1 und zeichnet die Informationen in der Datenbank auf.

Abbildung 26-1 Reihenfolge, in der der Task Server Tickle verarbeitet



Verwendung von Aufgaben, Jobs und Richtlinien

Aufgaben, Jobs und Richtlinien haben unterschiedliche Verwendungszwecke in Notification Server. Der jeweilige Verwendungszweck hängt davon ab, was Sie tun möchten.

Bei einer Richtlinie handelt es sich um einen Satz von Regeln, der auf einen Satz von Ressourcen angewendet wird (das so genannte Richtlinienziel). Eine Richtlinie kann basierend auf einem Zeitplan oder auf eingehenden Daten ausgewertet werden. Wenn eine Richtlinie ausgewertet wird, wird die entsprechende Aktion vorgenommen. Diese Aktion enthält im Allgemeinen ausgeführte Aufgaben auf den Zielressourcen, um sicherzustellen, dass sie alle der Richtlinie entsprechen. Mit einer Richtlinie können Sie Aktionen auf bestimmte Ressourcen, die Sie als Richtlinienziel definieren, anwenden.

Siehe "Informationen zu Symantec Management-Plattform-Richtlinien" auf Seite 393.

Eine Aufgabe ist eine separate Aktion ohne derzeit laufende Aktionen, die Sie auf ausgewählte Computer verteilen. Sie können Aufgaben basierend auf Ereignissen im System oder Änderungen in der Datenbank automatisch ausführen. Sie können Aufgaben auch automatisch ausführen, damit Computer weiterhin mit den Richtlinien konform sind.

Ein Job ist eine Folge von Aufgaben, die in einer bestimmte Reihenfolge ausgeführt werden.

Siehe "Informationen zu Task Management " auf Seite 426.

Verwenden Sie im Allgemeinen Richtlinien für die laufende Verwaltung und Aufgaben, um Richtlinien durchzusetzen oder einmalige Aktionen durchzuführen.

Tabelle 26-3 Verwendung von Aufgaben, Jobs und Richtlinien

Option	Kriterien
Aufgabe	Verwenden Sie eine Aufgabe, wenn die folgenden Kriterien zutreffend sind: ■ Sie müssen eine Aktion durchführen, die schnell fertig gestellt ist (keine laufenden Aktionen).
Job	Verwenden Sie einen Job, wenn die folgenden Kriterien zutreffend sind: ■ Sie müssen Aktionen in einer bestimmten Reihenfolge ausführen. ■ Eine Aktion kann nützlich sein, damit ein Benutzer eine Abfolge für eine Notification Server-Meldung erstellt oder daran gebunden ist.

Option	Kriterien
Richtlinie	Verwenden Sie eine Richtlinie, wenn die folgenden Kriterien zutreffend sind: ■ Sie haben statische Konfigurationsdaten, die an den Symantec Management-Agent gesendet werden sollen. ■ Sie haben laufende Aktionen ohne definitives Ende.

Informationen zu ausgeführten Aufgaben in der Hierarchie

Mit der Symantec Management-Plattform können Sie Aufgaben auf dem übergeordneten Notification Server erstellen und sie auf allen Clientcomputern in der Hierarchie ausführen. Diese Aufgaben werden ebenfalls auf den untergeordneten Notification Servern repliziert und können auf allen entsprechenden verwalteten Computer ausgeführt werden.

Siehe "Info zur Notification Server-Hierarchie" auf Seite 160.

Siehe "Informationen zu Task Management " auf Seite 426.

Beachten Sie beim Ausführen von Aufgaben in der Hierarchie die folgenden Besonderheiten für den Entwurf:

Clientcomputer melden Aufgabenstatusinformationen nur dem Notification Server, dem sie zugewiesen sind. Die Aufgabenstatusinformationen für die Clientcomputer, die einem untergeordneten Notification Server zugeordnet sind, sind auf dem übergeordneten Notification Server nicht immer präzise.

Wenn Sie eine Aufgabe auf dem übergeordneten Notification Server erstellen und sie auf allen Clientcomputern in der Umgebung ausführen, erstatten nicht alle Computer eine Rückmeldung an den übergeordneten Notification Server. Die Clientcomputer, die dem untergeordneten Notification Server zugeordnet sind, melden die Aufgabenstatusinformationen nur an den untergeordneten Notification Server. Außerdem werden die Aufgabenstatusinformationen vom untergeordneten Notification Server nicht zum entsprechenden übergeordneten Notification Server repliziert.

Daher werden auf der Seite "Aufträge/Aufgaben" am übergeordneten Notification Server die Aufgabenstatusinformationen für die Aufgaben, die auf den einem untergeordneten Notification Server zugewiesenen Clientcomputern ausgeführt werden, nicht präzise angezeigt.

Sie sehen die präzisen Aufgabenstatusinformationen für jeden Computer separat auf dem übergeordneten Notification Server im Fenster "Details der Aufgabeninstanz". Beachten Sie, dass durch das Fenster "Details der Aufgabeninstanz" eine URL des untergeordneten Notification Servers geöffnet wird und Sie die Identifikationsdaten des untergeordneten Notification Servers eingeben müssen.

Außerdem werden im Fenster "Details der Aufgabeninstanz" die richtigen Aufgabenstatusinformationen nur in den folgenden Fällen angezeigt:

- Wenn Sie eine Aufgabe auf dem übergeordneten Notification Server erstellen, klicken Sie auf "Schnellausführung" oder "Neuer Zeitplan > Jetzt" und fügen Sie Clientcomputer des untergeordneten Notification Servers als Ziel dieser Aufgabe hinzu.
- Wenn Sie eine Aufgabe auf dem übergeordneten Notification Server erstellen, fügen Sie einen Zeitplan für die Aufgabe hinzu und fügen Sie Clientcomputer des untergeordneten Notification Servers als Ziel dieser Aufgabe hinzu.

Wenn Sie die Aufgabe auf dem untergeordneten Notification Server replizieren und die Aufgabe von dort starten, können Sie die Aufgabenstatusdetails auf dem übergeordneten Notification Server anzeigen.

Der Serverauftrag, der Clientaufgaben enthält, wird vom übergeordneten Notification Server auf den entsprechenden untergeordneten Notification Server nicht ordnungsgemäß repliziert.	Wenn Sie einen Serverauftrag erstellen, der Clientaufgaben enthält, und ihn vom übergeordneten Notification Server auf den entsprechenden untergeordneten Notification Server replizieren, werden die Clientaufgaben in dem Serverauftrag auf den untergeordneten Notification Server abwärts repliziert, die Serveraufgaben und der Serverauftrag selbst jedoch nicht. Außerdem werden Serveraufgaben von diesem Auftrag auf dem übergeordneten Notification Server ausgeführt, während Clientaufgaben auf dem untergeordneten Notification Server ausgeführt werden. Um dieses Problem zu umgehen, können Sie einen Serverauftrag auf dem untergeordneten Notification Server erstellen und die replizierten Clientaufgaben dort hinzufügen. Außerdem können Sie einen Clientauftrag auf dem übergeordneten Notification Server erstellen. Der Clientauftrag, der Clientaufgaben enthält, wird ordnungsgemäß abwärts repliziert. Wenn Sie einen Clientauftrag, der Clientaufgaben enthält, vom übergeordneten Notification Server auf den untergeordneten Notification Server anwenden, ist der Auftragausführungsstatus nur auf dem übergeordneten Notification Server verfügbar. Auf dem untergeordneten Notification Server wird die Instanz dieses Auftrags nicht erstellt. Symantec empfiehlt nicht, einen Serverauftrag zu erstellen, der Clientaufgaben enthält. Weitere Informationen zu Aufträgen und Aufgaben erhalten Sie im folgenden Supportdatenbank-Artikel: http://www.symantec.com/docs/HOWTO9671
Wenn Sie die Aufgabe auf dem übergeordneten Notification Server löschen, wird durch die Option "Jetzt replizieren" diese Aufgabe auf dem untergeordneten Notification Server nicht gelöscht.	Wenn Sie eine Aufgabe auf dem übergeordneten Notification Server löschen und die Option "Jetzt replizieren" verwenden, um diesen Vorgang auf einem untergeordneten Notification Server zu replizieren, wird die Aufgabe auf dem untergeordneten Notification Server nicht gelöscht. Nur durch differenzielle oder vollständige Replikation wird die Aufgabe auf dem untergeordneten Notification Server erfolgreich gelöscht.

Bei Aufträgen, die nur Serveraufgaben enthalten, und für Serveraufgaben wird der Zeitplan vom übergeordneten auf den untergeordneten Notification Server nicht repliziert.	Wenn Sie eine neue Serveraufgabe auf dem übergeordneten Notification Server erstellen und planen und anschließend auf den untergeordneten Notification Server replizieren, wird der Zeitplan auf den untergeordneten Notification Server nicht repliziert. Sie müssen diese Aufgabe auf dem untergeordneten Notification Server separat planen.

Sequenzieren von Aufgaben

Mithilfe der Aufgabensequenzierung können Sie komplexe Verwaltungsvorgänge in einem einzelnen Job durchführen. Aufgaben können in einem Job sequenziell angeordnet werden, wodurch Sie höhere Flexibilität bei Ihrer Arbeit haben.

Siehe "Informationen zu Task Management " auf Seite 426.

Tabelle 26-4 Prozess für das Sequenzieren von Aufgaben

Schritt	Aktion	Beschreibung
Schritt 1	(Optionale) Verteilen von Task Servern	Mithilfe von Task Servern können Sie Ihre Jobs und Aufgaben auf Computer in Ihrem Netzwerk verteilen. Dann können die Jobs und Aufgaben auf verwalteten Computern ausgeführt werden. Symantec empfiehlt die Bereitstellung mindestens eines Task Servers pro Notification Server. Nachdem Sie den ersten zugehörigen Task Server bereitgestellt haben, fügen Sie zusätzliche Task Server für die nächsten 5000 bis 7500 Clientcomputer hinzu. Die Anzahl der verwalteten Computern, die ein Task Server verarbeiten kann, hängt von der Hardware des Task Server-Computers ab. Siehe "Bereitstellen eines Task Server" auf Seite 437.
Schritt 2	Erstellen einer Aufgabe	Aufgaben, die auf Notification Server oder verwalteten Computern ausgeführt werden. Siehe "Erstellen einer Aufgabe" auf Seite 438.
Schritt 3	Erstellen eines Jobs	Jobs führen Aufgaben, andere Jobs und Bedingungen aus. Siehe "Erstellen eines Jobs" auf Seite 439.

Schritt	Aktion	Beschreibung
Schritt 4	Ausführen von Aufträgen oder Aufgaben	Aufträge und Aufgaben können auf dem Notification Server oder verwalteten Computern ausgeführt werden. Siehe "Ausführen eines Auftrags oder einer Aufgabe mit Drag & Drop" auf Seite 441. Siehe "Ausführen eines Jobs oder einer Aufgabe" auf Seite 442. Siehe "Erneutes Ausführen einer fehlgeschlagenen Aufgabe" auf Seite 442. Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.
Schritt 5	Anzeigen des Echtzeitstatus der Aufträge oder Aufgaben	Sie können den Status des Auftrags oder der Aufgabe in der Symantec Management Console und auch auf einem Clientcomputer im Symantec Management Agent anzeigen. **Hinweis:** Der Status der Aufgabe wird in der Symantec Management Console alle fünf Minuten aktualisiert. Siehe "Anzeigen des Aufgabenstatus auf dem Symantec Management-Agent" auf Seite 445.

Bereitstellen eines Task Server

Mithilfe von Task Servern können Sie Aufträge und Aufgaben auf verschiedenen Computern im Netzwerk bereitstellen, auf denen Symantec Management-Agents die Aufträge und Aufgaben ausführen können. Wenn Sie Aufträge und Aufgaben verteilen, reduzieren Sie den Netzwerkverkehr und die Belastung des Notification Server. Der Symantec Management-Agent greift auf den ihm nächsten Task Server zu, um Aufträge und Aufgaben herunterzuladen.

Siehe "Task Management-Komponenten" auf Seite 428.

Jeder Notification Server wird zu einem Task Server, wenn die Task Server-Komponente installiert ist. Sie können dann bei Bedarf weitere Task Server verteilen.

Task Server kann nur auf einem Computer installiert werden, auf dem IIS installiert ist.

Folgende Anforderungen gelten für einen Task Server-Computer:

- Microsoft .NET Framework 3.5
- Betriebssystem: Windows XP x86 SP3, Windows x64 SP2 oder Windows Server 2003 SP2
- Microsoft Internet Information Services (IIS)
- Symantec Management-Agent

Empfohlene Hardwareanforderungen für einen Task Server-Computer:

- Prozessor: Intel Pentium 4 oder Äquivalent
- 1 GB RAM
- 1 GB Speicherplatz

Symantec empfiehlt die Bereitstellung mindestens eines Task Servers pro Notification Server. Nachdem Sie den ersten zugehörigen Task Server bereitgestellt haben, fügen Sie zusätzliche Task Server für die nächsten 5000 bis 7500 Clientcomputer hinzu. Die Anzahl verwalteter Computer, die ein Task Server verarbeiten kann, hängt von der Hardware des Task Server-Computers ab.

Siehe "Info zu Site Services" auf Seite 133.

Diese Aufgabe ist ein Schritt beim Sequenzieren von Aufgaben.

Siehe "Sequenzieren von Aufgaben" auf Seite 436.

So verteilen Sie einen Task Server mithilfe der Site-Services

- Verteilen Sie einen Task Server als Site-Server.

  Siehe "Verwalten von Site Servers" auf Seite 137.

Erstellen einer Aufgabe

Mithilfe vordefinierter Aufgabentypen erstellen und implementieren Sie Aufgaben auf verwalteten Computern. Der von Ihnen gewählte Aufgabentyp hängt davon ab, was Sie tun möchten. Viele Aufgabentypen stehen im Fenster "Task Management" zur Verfügung. Einige Symantec liefern Lösungen auch Aufgabentypen und Beispiejobs.

Diese Aufgabe ist ein Schritt beim Sequenzieren von Aufgaben.

Siehe "Sequenzieren von Aufgaben" auf Seite 436.

So erstellen Sie eine Aufgabe

1. Klicken Sie in Symantec Management Console im Menü "Verwalten" auf "Jobs und Aufgaben".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, in dem die Aufgabe erstellt werden soll, und wählen Sie im Kontextmenü die Option "Neu > Aufgabe".
3. Wählen Sie im Dialogfeld "Neue Aufgabe erstellen" im linken Teilfenster den Aufgabentyp aus.
4. Konfigurieren Sie die Aufgabe im rechten Teilfenster.
5. Klicken Sie auf "OK".

Erstellen eines Jobs

Sie können Jobs erstellen, die mehrere Aufgaben oder Jobs ausführen. Die zwei Typen von Jobs sind Serverjobs und Clientjobs. Serverjobs werden auf Notification Server ausgeführt. Clientjobs werden durch einen Task Server auf verwalteten Computern implementiert. Der verwaltete Computer führt anschließend den Job aus und erstattet Notification Server eine Rückmeldung.

Jobs können mehrere Aufgaben, mehrere Jobs und mehrere Bedingungen enthalten, wodurch Sie hohe Flexibilität beim Einrichten der erforderlichen Jobfolge haben.

Diese Aufgabe ist ein Schritt beim Sequenzieren von Aufgaben.

Siehe "Sequenzieren von Aufgaben" auf Seite 436.

So erstellen Sie einen Auftrag

1. Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Aufträge und Aufgaben".
2. Im linken Teilfenster klicken Sie mit der rechten Maustaste auf den Ordner, in dem die Aufgabe erstellt werden soll, und wählen dann im Kontextmenü die Option "Neu > Serverauftrag" bzw. "Neu > Clientauftrag".
3. Konfigurieren Sie im rechten Teilfenster den Auftrag:

Bearbeiten Sie den Namen des Auftrags.	Klicken Sie auf den Namen und geben Sie einen neuen ein.

Erstellen einer neuen Aufgabe, die einem Auftrag hinzugefügt werden soll	1 Klicken Sie auf "Neu" > "Aufgabe". 2 Wählen Sie im Dialogfeld "Neue Aufgabe erstellen" im linken Teilfenster eine Aufgabe aus. 3 Konfigurieren Sie die Aufgabe im rechten Teilfenster. 4 Klicken Sie auf "OK".
Hinzufügen einer vorhandene Aufgabe bzw. eines Auftrags zu einem Auftrag	1 Klicken Sie auf "Vorh. hinzufügen". 2 Wählen Sie im Dialogfeld "Vorhandene Aufgabe hinzufügen" im linken Teilfenster die Aufgabe oder den Job aus, die/den Sie hinzufügen möchten. 3 Klicken Sie auf "OK". Sie können die Reihenfolge der Aufgaben bzw. Aufträge, die einem Auftrag hinzugefügt werden, per Drag&Drop ändern. Sie können Aufgaben, Aufträge und Bedingungen auch mit den Pfeilschaltflächen verschieben.
Hinzufügen einer Bedingung zu einem Auftrag	1 Wählen Sie "Neu" > "Bedingung". 2 Im Dialogfeld "Bedingung bearbeiten" enthält die Regel eine "Wo" -Klausel, mit der Sie eine Aufgabe bzw. einen Auftrag, einen auszuführendem Vorgang und eine Bedingung zum Ausführen des Vorgangs auf die Aufgabe bzw. den Auftrag auswählen können. 3 Wählen Sie in der ersten Dropdown-Liste die Aufgabe bzw. den Auftrag und den Rückgabecode für die Bedingung aus bzw. geben Sie sie/ihn ein. 4 In der zweiten Dropdown-Liste wählen Sie den Vorgang aus, den die Regel ausführen soll. 5 Im dritten Feld geben Sie die Bedingung ein. 6 (Optional) Sie können weitere Regeln hinzufügen, indem Sie auf "Regel hinzufügen" klicken. 7 Klicken Sie auf "OK". Sie können Aufgaben oder Aufträge hinzufügen, die entsprechend der Bedingung unter "Sonst" ausgeführt werden sollen.

4 Klicken Sie auf "Änderungen speichern".

Ausführen eines Auftrags oder einer Aufgabe mit Drag & Drop

In der erweiterten Ansicht "Aufträge/Aufgaben" können Sie die Aufträge und Aufgaben leicht anzeigen, ausführen und planen.

Siehe "Informationen zur Ansicht Jobs/Aufgaben " auf Seite 44.

Sie können Aufträge und Aufgaben auch starten, indem Sie sie auf einen oder mehrere Computer ziehen und ablegen. Sie können auch die Option "Schnellausführung" verwenden, um einen Auftrag oder eine Aufgabe ohne einen manuellen Drilldown zu bearbeiten.

Siehe "Festlegen der Ziele für Richtlinien oder Aufgaben" auf Seite 396.

Hinweis: Eine der folgenden Lösungen oder Suites muss installiert sein, damit diese Aufgabe ausgeführt wird: Deployment Solution (eigenständiges Produkt), IT Management Suite, Server Management Suite oder Client Management Suite.

So führen Sie einen Job oder eine Aufgabe mit Drag & Drop aus

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Aufträge und Aufgaben".
2. Klicken Sie im Navigationsbereich auf den Auftrag oder die Aufgabe, die Sie ausführen möchten, und ziehen Sie sie nach rechts, um den Drag & Drop-Vorgang zu initiieren.

   Die Ergebnisse Ihrer aktuellsten Computersuche erscheinen im Listenbereich. Wenn Sie Ihre letzte Computersuche gefiltert haben, werden die Ergebnisse der gefilterten Suche in der Liste angezeigt.

   Siehe "Suchen nach einem Computer und Speichern der Suche als Filter" auf Seite 39.
3. Um die Computer zu auswählen, auf denen Sie den Auftrag oder die Aufgabe ausführen möchten, führen Sie eine der folgenden Schritte aus:
   - Um den Auftrag oder die Aufgabe auf allen aufgeführten Computern auszuführen, legen Sie sie auf das Namenssymbol im Listenbereich ab.
   - Um den Auftrag oder die Aufgabe auf einem bestimmten Computer auszuführen, legen Sie sie auf dem Computer in der Liste ab.
   - Um den Auftrag oder die Aufgabe auf einer gespeicherten Suche, Organisationsansicht oder Organisationsgruppe auszuführen, ziehen Sie sie auf die Blade "Computer" und legen Sie sie dann auf eine gespeicherte Suche, eine Organisationsansicht oder eine Organisationsgruppe ab.

4 Geben Sie im Dialogfeld "Neuer Zeitplan" den Zeitplan des Auftrags oder der Aufgabe, an und klicken Sie dann auf "Zeitplan".

Ausführen eines Jobs oder einer Aufgabe

Die von Ihnen erstellten Jobs und Aufgaben können auf Notification Server oder verwalteten Computern abhängig davon ausgeführt werden, ob es sich um Server- oder Clientaufgaben handelt. Serveraufgaben sind die Aufgaben, die auf einem Notification Server-Computer ausgeführt werden. Clientaufgaben sind die Aufgaben, die auf einem Clientcomputer ausgeführt werden.

Wenn mehr als eine Aufgabe einem Job hinzugefügt wird, werden sie nacheinander durchgeführt. Wenn eine Bedingung hinzugefügt wird, basieren die Aufgaben, die durchgeführt werden, auf den Ergebnisse der Bedingung. Der Server muss den Status einer vorherigen Aufgabe empfangen, die abgeschlossen wurde, bevor er die nächste Aufgabe im Job startet. Es gibt unter Umständen eine Verzögerung von wenigen Sekunden, bevor die nächste Aufgabe gestartet wird.

Diese Aufgabe ist ein Schritt beim Sequenzieren von Aufgaben.

Siehe "Sequenzieren von Aufgaben" auf Seite 436.

So führen Sie einen Job oder eine Aufgabe aus

1 Klicken Sie in Symantec Management Console im Menü "Verwalten" auf "Jobs und Aufgaben".

2 Wählen Sie im linken Teilfenster den Job oder die Aufgabe aus, den/die Sie ausführen möchten.

3 Fügen Sie einen Zeitplan für die Ausführung des Jobs oder der Aufgabe hinzu.

Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.

Erneutes Ausführen einer fehlgeschlagenen Aufgabe

Sie können eine Aufgabe bei fehlgeschlagenen Computern erneut ausführen.

Siehe "Informationen zu Task Management " auf Seite 426.

Die Aufgabe kann wie folgt erneut ausgeführt werden:

- Sie können mehrere Aufgabeninstanzen für eine erneut Ausführung auswählen. Alle fehlgeschlagenen Computer der enthaltenen Aufgabeninstanzen sind in der Aufgabeninstanz für die erneute Ausführung enthalten.
- Sie können nur fehlgeschlagene Clientaufgaben erneut ausführen, nicht Serveraufgaben.

- Durch "Fehlgeschlagene erneut ausführen" werden alle Ziele ignoriert, die in der vorherigen Aufgabeninstanz verwendet wurden, unabhängig von der Art der Erstellung (Schnellausführung, Planung durch Computerliste oder Planung durch Ziel). Die erneute Ausführung erfolgt anhand der Liste der fehlgeschlagenen Computer von der soeben ausgeführten Aufgabe.

Hinweis: Verwenden Sie die Funktion für die erneute Ausführung nur auf der untergeordneten Ebene des Notification Servers, auf der Sie die Aufgabenstatusanzeigen sehen. Es wird empfohlen, dass Sie Aufgaben vom übergeordneten Notification Server in der Hierarchie nicht erneut ausführen, da eine zeitliche Verzögerung beim Replizieren der Daten auftreten kann.

So führen Sie eine fehlgeschlagene Aufgabe erneut aus

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Computer".

   Hinweis: Sie können direkt "Verwaltung > Aufträge und Aufgaben" aufrufen und die Schritte 2 und 3 überspringen.

   ---

2. Klicken Sie auf die Doppelpfeile (>>) am oberen Rand des Listenbereichs, um die Container-Übersicht "Software Delivery" aufzurufen.
3. Klicken Sie unter "Schnellverteilungsaufgaben" auf eine Aufgabeninstanz, die auf einigen Computern fehlgeschlagen ist und die Sie auf diesen Computern erneut ausführen möchten.
4. Klicken Sie im Teilfenster "Aufgabenstatus" auf "Fehlgeschlagene erneut ausführen", um die Aufgabeninstanz(en) in der Liste der Computer auszuführen, die den Status "Fehlgeschlagen" zurückgegeben haben.
5. Dadurch wird das Fenster "Neuer Zeitplan" aufgerufen. Das Feld "Ausgewählte Geräte" enthält bereits die Computer, auf denen die Aufgabeninstanz(en) nicht ausgeführt werden konnte(n).

   Hinweis: Wenn Sie bei einer Aufgabeninstanz ohne fehlgeschlagene Computer auf "Fehlgeschlagene erneut ausführen" klicken, werden Sie in einer Popup-Meldung informiert, dass keine fehlgeschlagenen Computer für diese Aufgabeninstanz vorhanden sind. Wenn Sie bei einer Aufgabeninstanz, die sich im ausstehenden oder auszuführenden Status befindet, auf "Fehlgeschlagene erneut ausführen" klicken, werden keine Computer aufgeführt, da die Aufgabe weder als erfolgreich noch als fehlgeschlagen ausgeführt wurde.

   ---

6 Klicken Sie auf "Zeitplan", um die erneute Ausführung der Aufgabe auf den fehlgeschlagenen Computern zu planen.

Dadurch wird eine neue Instanz der Aufgabe erstellt. Die ältere Instanz ist weiterhin vorhanden.

Hinweis: Möglicherweise wird eine Fehlermeldung ähnlich der folgenden angezeigt: "Dieser Aufgabendurchlauf wurde gelöscht und kann weder angezeigt noch erneut ausgeführt werden. Es sind nur Zusammenfassungsdaten vorhanden." Task Management verfügt über eine tägliche Bereinigungsaufgabe, die je nach Benutzereinstellung ausgeführt wird, um die Anzahl der Arbeitszeilen in der Datenbank zu beschränken. Dadurch wird verhindert, dass sich die Leistung von Task Management zu sehr verringert. Die Bereinigungsaufgabe speichert am Ende des Tages nur die 200.000 letzten Aufgabeninstanzen. Die Computeranzahl zeigt weiterhin alle Computer an, für die die Aufgabe ausgeführt wurde. Wenn jedoch die Details einer dieser Aufgabeninstanzen gelöscht wurden, sind diese Aufgaben bei "Fehlgeschlagene erneut ausführen" nicht enthalten. Dies kann zu unterschiedlichen Werten bei Anzahl der Computer, auf denen die Aufgabe fehlgeschlagen ist, und Anzahl beim Klicken auf "Fehlgeschlagene erneut ausführen" führen.

---

7 Dieser neue Zeitplan wird jetzt auf der Flipbook-Seite "Software Delivery" angezeigt. Sie können sehen, welche Instanz der Aufgabe kürzlich ausgeführt oder erneut ausgeführt wurde. Außerdem sehen Sie, auf wie vielen Computern die Aufgabe erfolgreich oder nicht erfolgreich ausgeführt wurde.

Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag

Wenn Sie die Ausführung einer Richtlinie, Aufgabe oder eines Jobs planen, haben Sie zwei Optionen: Schnellausführung und Zeitplan. Die Schnellausführungsoption führt die aktuelle Richtlinie, Aufgabe oder den Job sofort auf dem angegebenen Computer aus. Die Zeitplanoption stellt mehrere Planungs- und Zielcomputeroptionen bereit. Mit der Zeitplanoption können Sie einen Zeitplan einstellen. Das Ziel muss anderswo definiert werden.

So fügen Sie einen Zeitplan zur Schnellausführung hinzu

1 Klicken Sie in Symantec Management Console im Menü "Verwalten" auf "Jobs und Aufgaben".

2 Wählen Sie im linken Teilfenster die Richtlinie, den Job oder die Aufgabe aus, auf die Sie die Schnellausführungsoption anwenden möchten.

3 Klicken Sie im rechten Teilfenster unter "Aufgabenstatus" auf "Schnellausführung".

4 Wählen Sie im Dialogfeld "Jetzt schnell ausführen" den Namen des Computers aus, auf dem Sie die Richtlinie, Aufgabe oder den Job ausführen möchten.

5 Klicken Sie auf "Ausführen".

So fügen Sie einen neuen Zeitplan hinzu

1 Klicken Sie in Symantec Management Console im Menü "Verwalten" auf "Jobs und Aufgaben".

2 Wählen Sie im linken Teilfenster die Richtlinie, den Job oder die Aufgabe aus, die Sie planen möchten.

3 Klicken Sie im rechten Teilfenster unter "Aufgabenstatus" auf "Neuer Zeitplan".

4 Konfigurieren Sie den Zeitplan im Dialogfeld "Neuer Zeitplan".

5 Klicken Sie auf "Zeitplan".

Wenn Aufgaben oder Jobs zur Ausführung markiert sind, erscheinen sie im Abschnitt "Job- und Aufgabenstatus".

Anzeigen des Aufgabenstatus auf dem Symantec Management-Agent

Der Aufgabenstatus (einschließlich Aufgabenverlauf) wird auf Symantec Management Agent registriert. Starten Sie zum Anzeigen des Aufgabenstatus auf einem Computer den Symantec Management-Agent. Der Aufgabenstatus gibt Einblick in die ausgeführten Aufgaben und ihre Ergebnisse.

Diese Aufgabe ist ein Schritt beim Sequenzieren von Aufgaben.

Siehe "Sequenzieren von Aufgaben" auf Seite 436.

So zeigen Sie den Aufgabenstatus im Symantec Management-Agent an

1 Doppelklicken Sie auf dem Computer, auf dem der Status angezeigt werden soll im Infobereich auf das Symbol zum Öffnen des Symantec Management-Agent.

2 Klicken Sie im Dialogfeld "Symantec Management-Agent" auf die Registerkarte "Aufgabenstatus".

Anzeigen und Bearbeiten von Berechtigungen für einen Aufgabentyp

Sie können die Berechtigungen für die Eigenschaften von Aufgabentypen anzeigen und bearbeiten. Änderungsberechtigungen für den Aufgabentyp ermöglichen Ihnen

eine Kontrolle darüber, welche Benutzer neue Aufgaben erstellen können. Benutzer, die die Berechtigung zum Erstellen neuer Aufgaben haben, können neue Aufgaben dieses Typs erstellen.

Siehe "Informationen zu Task Management " auf Seite 426.

Siehe "Sequenzieren von Aufgaben" auf Seite 436.

Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.

Siehe "Task Server-Berechtigungen" auf Seite 528.

So zeigen Sie Berechtigungen eines Aufgabentyps an und bearbeiten sie

1. Klicken Sie in Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Klicken Sie im linken Teilfenster auf "Notification Server" > "Aufgabeneinstellungen" > "Aufgabentypen".
3. Navigieren Sie zum Aufgabentyp, den Sie anzeigen möchten, und klicken Sie darauf.
4. Klicken Sie im rechten Teilfenster auf "Berechtigungen anzeigen".
5. Um Berechtigungen zu bearbeiten, bearbeiten Sie im Sicherheitsrollenmanager die Berechtigungen für den Aufgabentyp.

   Siehe "Zuweisen von Sicherheitsberechtigungen zu Ordnern und Elementen" auf Seite 108.

Erstellen von Aufgaben für die Eingabe oder Ausgabe von Aufgabeneigenschaften

Eingabeeigenschaften sind die Eigenschaften, die aus einer Quelle an eine Aufgabe weitergeleitet werden. Aufgaben können Eingabeeigenschaften von einem festgelegten Wert, von anderen Aufgaben oder bei Laufzeit erhalten. Aufgaben können diese Eingabeeigenschaften (ähnlich Variablen) verwenden, um ihre Funktionen auszuführen. Alle Eigenschaften, die für eine Aufgabe (Eingabeeigenschaften sowie Eigenschaften, die die Aufgabe erstellt) zur Verfügung stehen, werden als Aufgabeneigenschaften bezeichnet.

Eine Aufgabe kann ihre Aufgabeneigenschaften an andere Aufgaben ausgeben. Wenn Sie eine Aufgabe haben, die Eigenschaften ausgibt, kann jede folgende Aufgabe in diesem Job jene Ausgabeeigenschaften für ihre Eingabeeigenschaften verwenden. Die Aufgaben müssen nicht gleichzeitig ausgeführt werden.

Sie benötigen keine ausgegebene Aufgabe für jede eingegebene Aufgabe. Eingegebene Aufgaben können auch Eingaben von einem festgelegten Wert oder bei Laufzeit erhalten.

Siehe "Informationen zu Task Management " auf Seite 426.

Siehe "Erstellen einer Aufgabe" auf Seite 438.

So erstellen Sie eine Aufgabe, die Eigenschaften ausgibt

1. Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Aufträge und Aufgaben".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, in dem die Aufgabe erstellt werden soll, und wählen Sie im Kontextmenü die Option "Neu > Aufgabe".
3. Wählen Sie im Dialogfeld "Neue Aufgabe erstellen" im linken Teilfenster eine Aufgabe mit einer Option aus der Kategorie "Erweitert" (z. B. "Skript ausführen").
4. Klicken Sie im rechten Teilfenster auf "Erweitert".
5. Aktivieren Sie das Kontrollkästchen "Skriptausgabe mit Aufgabenstatus speichern" und klicken Sie dann auf "OK".

   Wenn dieses Kontrollkästchen für eine Aufgabe aktiviert ist, werden alle seine Aufgabeneigenschaften angezeigt und stehen nachfolgenden Aufgaben in einem Auftrag zur Verfügung.
6. Konfigurieren Sie die Aufgabe.
7. Klicken Sie im Dialogfeld "Neue Aufgabe erstellen" auf "OK".

So erstellen Sie eine Aufgabe, die Eingabeeigenschaften von einer anderen Aufgabe erhält

1. Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Aufträge und Aufgaben".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, in dem die Aufgabe erstellt werden soll, und wählen Sie im Kontextmenü die Option "Neu > Aufgabe".
3. Wählen Sie im Dialogfeld "Neue Aufgabe erstellen" im linken Teilfenster eine Skriptaufgabe aus.

   Skriptaufgaben erhalten Eingabeeigenschaften.
4. Um diese Aufgabe zum Übergeben der Eigenschaften an eine andere Aufgabe zu verwenden, klicken Sie auf "Erweitert", aktivieren das Kontrollkästchen "Skriptausgabe mit Aufgabenstatus speichern" und klicken auf "OK".

5 Geben Sie im Dialogfeld "Neue Aufgabe erstellen" im Abschnitt "Skriptbefehl" einen oder mehrere Token ein (z. B. `%!input!%`), die die Ausgabe erfassen.

6 Klicken Sie auf "OK".

So richten Sie Aufgaben innerhalb eines Jobs für die Eingabe ein

1 Erstellen Sie einen Auftrag und legen darin die Aufgaben ab, die Sie für Ausgabe und Eingabe erstellt haben. Jede ausgegebene Aufgabe muss der Aufgabe vorausgehen, die ihre Ausgabe erhält.

Siehe "Erstellen eines Jobs" auf Seite 439.

2 Konfigurieren Sie jede eingegebene Aufgabe im Job.

Das Fenster "Aufgabeneingabe" wird auf der rechten Seite angezeigt, wenn Sie in folgenden Situationen auf die Aufgabe klicken: wenn eine Clientaufgabe eine Eingabe aufweist und sich in einem Client- bzw. Serverauftrag befindet.

Zur Aufgabeneingabe auffordern, immer wenn dieser Job ausgeführt wird	Wählen Sie diese Option aus, um die Eingabe manuell einzugeben, wenn der Job ausgeführt wird.

Aufgabeneingabe jetzt eingeben	Aktivieren Sie diese Option, um die Aufgabeneingabe zu diesem Zeitpunkt einzugeben: ■ einen bestimmten Wert verwenden Wählen Sie diese Option aus, um einen Wert zu verwenden, der sich nicht ändert. Geben Sie den Wert in das Feld ein, das bei Aktualisierung des Bildschirms angezeigt wird. Wenn diese Aufgabe eine Clientaufgabe innerhalb eines Serverjobs ist, müssen Sie den Computer oder die Computer auswählen, auf dem/denen die Clientaufgabe ausgeführt wird. Alle Clientaufgaben haben diesen Parameter als Standardeingabeparameter, wenn sie sich innerhalb von Serverjobs befinden. ■ Ausgabe von vorheriger Aufgabe verwenden Wählen Sie diese Option aus, um die Ausgabe einer vorherigen Aufgabe zu verwenden. Verwenden Sie diesen Parameter, wenn es eine ausgegebene Aufgabe in diesem Job gibt, den Sie verwenden möchten. Wenn der Bildschirm aktualisiert wird, wird der Variablenname sowie eine Liste der verfügbaren ausgegebenen Aufgaben angezeigt. Wählen Sie die Aufgabe aus, deren Ausgabe Sie für diese Aufgabe verwenden möchten. ■ Zur Laufzeit abfragen Wählen Sie diese Option aus, um bei Laufzeit zur Eingabe aufgefordert zu werden.

3 Klicken Sie auf "OK".

Bereinigen von Aufgabendaten

Um die Last auf Ihren Systemressourcen zu verringern, können Aufgabendaten unter Verwendung von Reinigungsoptionen archiviert oder gelöscht werden.

Siehe "Informationen zu Task Management " auf Seite 426.

Siehe "Sequenzieren von Aufgaben" auf Seite 436.

So bereinigen Sie Aufgabendaten

1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".

2 Klicken Sie im linken Teilfenster auf "Notification Server" > "Aufgabeneinstellungen" > "Aufgabendaten bereinigen".

3 Bearbeiten Sie auf der Seite "Aufgabendaten bereinigen" die erforderlichen Details.

Jeden Abend werden die aktuellen Aufgabendaten und archivierten Aufgabendaten den folgenden Einstellungen entsprechend verschoben oder gelöscht.

Maximale Anzahl von Datenbankarbeitszeilen	Nachdem die Anzahl aktiver Datenbankzeilen die Höchstzahl erreicht, werden die ältesten Zeilen archiviert, bis die Höchstzahl nicht mehr überschritten ist. Datenbankarbeitszeilen sind die Datenbankzeilen, die vor Kurzem verwendet wurden. Wir empfehlen, diese Zahl klein zu halten, um die Last auf die Systemressourcen zu reduzieren.
Bereinigung nach Bedarf ausführen:	Wenn Sie diese Option wählen und die Anzahl verwendeter Zeilen überschritten wird, wird die Bereinigungsaufgabe sofort gestartet.

4 (Optional) Fügen Sie einen Zeitplan hinzu, um die Aufgabendaten zu bereinigen.

Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.

5 Klicken Sie auf "Änderungen speichern".

Bereinigen von Aufgabenversionsdaten

Um die Auslastung der Systemressourcen zu verringern, kann der Aufgabenversionsverlauf mithilfe von Bereinigungsoptionen archiviert oder gelöscht werden.

Siehe "Informationen zu Task Management " auf Seite 426.

Siehe "Sequenzieren von Aufgaben" auf Seite 436.

So räumen Sie Aufgabenversiondaten auf

1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".

2 Klicken Sie im linken Teilfenster auf "Notification Server > Aufgabeneinstellungen > Versionsdaten bereinigen".

3 Bearbeiten Sie auf der Seite "Versionsdaten bereinigen" die erforderlichen Details.

Standardmäßig werden einmal pro Woche die Aufgabenversionen entsprechend den folgenden Einstellungen gelöscht.

Maximale Anzahl Aufgabenversionen zur Speicherung in der Datenbank	Wenn die Anzahl von Versionen die ausgewählte Zahl erreicht, werden die ältesten Versionen gelöscht, um die Datenbankleistung zu verbessern. Sie können auswählen, ob 1, 5, 10 oder 20 Versionen einer Aufgabe in der Datenbank gespeichert werden.

4 (Optional) Fügen Sie einen Zeitplan hinzu, um die Aufgabendaten zu bereinigen.

Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.

5 Klicken Sie auf "Änderungen speichern".

Ändern der Client Task Agent-Einstellungen

Der Client Task Agent ist Teil des Symantec Management-Agent. Er empfängt Jobs und Aufgaben vom Task Server und führt sie auf verwalteten Computern aus. Dann erstattet er dem Notification Server eine Rückmeldung.

Hinweis: Wenn Sie den Symantec Management-Agent auf einem Computer installieren, gibt es eine Verzögerung, bevor der Client Task Agent auf dem Notification Server registriert wird. Alle Aufgaben, die während dieser Zeit (gewöhnlich ca. 10 Minuten) diesen Computer als Ziel haben, werden in die Warteschlange gestellt, bis der Client Task Agent registriert wurde. Nachdem der Client Task Agent registriert wurde, werden die Aufgaben sofort ausgeführt.

Hinweis: Normalerweise öffnet der Client Task Agent eine Direktverbindung zum Task Server auf Port 50124. Der Task Server verwendet diese Verbindung, um dem Agent mitzuteilen, wenn neue Aufgaben verfügbar sind. Wenn jedoch ein Proxy verwendet wird, ist keine Direktverbindung möglich, also kann der Task Server dem Agenten nicht mitteilen, wenn neue Aufgaben verfügbar werden. Um auf dem aktuellen Stand zu bleiben, müssen Sie den entsprechenden Wert "Task Server auf neue Aufgaben prüfen" im Feld "Aufgabe aktualisieren" festlegen.

Siehe "Informationen zu Task Management " auf Seite 426.

Siehe "Sequenzieren von Aufgaben" auf Seite 436.

Siehe "Task Management-Komponenten" auf Seite 428.

Sie können Client Task Agent-Einstellungen ändern, um die Leistungsfähigkeit zwischen dem Client Task Agent und dem Task Server zu verbessern. Um die Leistungsfähigkeit zu verbessern, können Sie das Zeitintervall festlegen, mit dem der Client Task Agent Aufgaben vom Task Server anfordern soll. Sie können die Standardmethode definieren, mit der der Notification Server einen Task Server auswählt. Außerdem können Sie die Aktion festlegen, die ausgeführt werden soll, falls mehrere Task Server an einem Standort verfügbar sind.

So ändern Sie Client Task Agent-Einstellungen

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Klicken Sie im linken Teilfenster auf "Notification Server" > "Aufgabeneinstellungen" > "Task Agent-Einstellungen".
3. Bearbeiten Sie auf der Seite "Task Agent-Einstellungen" die erforderlichen Details.

Task Server auf neue Aufgaben prüfen alle	Das Intervall in Minuten, in dem der Agent Aufgaben vom Task Server anfordern soll.
Wenn mehrere Task Server an einer Site verfügbar sind	Die auszuführende Aktion, falls mehrere Task Server in einer Site verfügbar sind.

4. Wählen Sie die Ziele, Computer oder Benutzer, auf die die Änderungen angewandt werden sollen.
5. Klicken Sie auf "Änderungen speichern".

Zugriff auf das Job- und Aufgabenportal

Das Job- und Aufgabenportal ermöglicht das Erstellen und Planen von Aufgaben, damit diese auf Ihren verwalteten Ressourcen ausgeführt werden. Sie können über die Symantec Management Console auf das Job- und Aufgabenportal zugreifen.

Über das Portal "Aufträge und Aufgaben" erhalten Sie einfachen Zugriff auf die meisten Auftrags- und Aufgabenaktionen der Aufgabenverwaltung.

Mehrere Web-Parts stehen auf dieser Seite zur Verfügung:

Schnellstart – Aufträge und Aufgaben	Damit können Sie Aufträge und Aufgaben erstellen, ausführen oder planen.

Task Server	Damit können Sie Ihre Task Server anzeigen und wie viele Clientcomputer mit jedem Task Server verbunden sind.
Aufgabencomputer und -geräte	Damit können Sie Ihre Task Server und verwalteten Computer anzeigen.

Sie können die Seite auch so konfigurieren, dass nur die von Ihnen gewünschten Web-Parts angezeigt werden. Mithilfe der Schaltfläche "Bearbeiten" in der rechten oberen Ecke können Sie die Web-Parts ändern, die in diesem Portal angezeigt werden.

So greifen Sie auf das Job und Aufgabenportal zu

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Konsole > Portalseiten".
2. Im linken Teilfenster klicken Sie auf "Job- und Aufgabenportal".
3. (Optional) Klicken Sie im Portal "Aufträge und Aufgaben" in dem Web-Part, den Sie aktualisieren möchten auf das Symbol "Aktualisieren".

   Wenn Sie eine automatische Aktualisierung für einen Web-Part einrichten möchten, klicken Sie auf das Symbol "Aktualisieren", aktivieren Sie das Kontrollkästchen "Aktualisieren alle" und klicken Sie anschließend in der Dropdown-Liste auf den gewünschten Zeitabstand der Aktualisierung.

Kapitel 27

Verwenden des Ressourcenmanagers

In diesem Kapitel werden folgende Themen behandelt:

- Informationen zur Ressourcenverwaltung
- Zugreifen auf Ressourcenmanager
- Anzeigen der Inventardaten für eine Datenklasse
- Anzeigen der Ereignisdaten für eine Datenklasse
- Hinzufügen einer Ressource zu einer Organisationsgruppe
- Ressourcenmanager-Aufgaben

Informationen zur Ressourcenverwaltung

Mit dem Ressourcenmanager können Sie die Ressourcen in Configuration Management Database (CMDB) verwalten. Im Ressourcenmanager können Sie Informationen anzeigen und zahlreiche Aufgaben an einer Ressource durchführen. Die verfügbaren Informationen und Aufgaben, die Sie durchführen können, hängen vom Typ der gewählten Ressource ab.

Wenn Sie auf den Ressourcenmanager zugreifen, wird die Portalseite für Basisressource für alle Ressourcen ausgenommen Computer und Softwarepakete angezeigt. Für eine Computerressource oder ein Softwarepaket wird die Seite "Ressourcenmanager" angezeigt. Die Seite, auf der Ressourcen, bei denen es sich nicht um Computerressourcen handelt, angezeigt werden, enthält den Web-Part "Elementeigenschaft – Übersicht". Dieser Web-Part zeigt Eigenschaftsinformationen zur ausgewählten Ressource an (z. B. GUID und Produktname). Für eine Computerressource zeigt die Seite eine Übersicht an. Wenn Sie auf

"Ressourcenmanager-Portal" im Menü "Startseite" klicken, können Sie auf den Web-Part "Elementeigenschaft – Übersicht" für eine Computerressource zugreifen.

Siehe "Ressourcenmanager-Aufgaben" auf Seite 457.

Sie können auf Ressourcenmanager auf verschiedene Weise zugreifen. Durch die verschiedenen Methoden ist es einfach, auf Ressourcenmanager zuzugreifen, unabhängig davon, wo Sie sich in Symantec Management Console befinden.

Siehe "Zugreifen auf Ressourcenmanager" auf Seite 455.

Zugreifen auf Ressourcenmanager

Sie können auf Ressourcenmanager auf die folgenden Weisen zugreifen:

- Über das Menü "Verwalten" der Symantec Management Console
- Über einen Rechtsklick auf eine Ressource in einer Liste oder einem Bericht
- Doppelklicken auf eine Ressource in einer Liste oder einen Bericht
- Eingeben einer URL in den Webbrowser

Siehe "Informationen zur Ressourcenverwaltung" auf Seite 454.

So greifen Sie über das Menü "Verwalten" auf den Ressourcenmanager zu

1. Klicken Sie in der Symantec Management Console im Menü "Verwalten" auf "Ressource".
2. Wählen Sie im Dialogfeld "Ressource auswählen" die Ressource aus, die Sie verwalten möchten, und klicken Sie dann auf "OK".

   Die Seite "Ressourcenmanager" wird mit Übersichtsinformationen über die ausgewählte Ressource geöffnet.

So greifen Sie auf Ressourcenmanager über einen Rechtsklick zu

- Klicken Sie mit der rechten Maustaste in einer Liste der Ressourcen oder in einem Bericht innerhalb der Symantec Management Console auf die gewünschte Ressource und wählen Sie "Ressourcenmanager".

  Einige in den Listen, Ressourcen oder Berichten ist die Rechtsklickoption für Ressourcenmanager evtl. nicht verfügbar. Verwenden Sie in diesen Fällen eine der anderen Methoden, um auf Ressourcenmanager zuzugreifen.

So greifen Sie durch Doppelklicken auf eine Ressourcen auf den Ressourcenmanager zu

- In einer Liste von Ressourcen oder in einem Bericht in der Symantec Management Console doppelklicken Sie auf die Ressource, die Sie verwalten möchten.

So greifen Sie Ressourcenmanager über eine URL zu

- Geben Sie in einem Browserfenster folgende URL ein:

  http://*NS-Name*/Altiris/Console/Dashboard/DashboardView.aspx?name=*Name der Zielressource*

  NS-Name ist der Name des Notification Server-Computers. *Name der Zielressource* kann der Ressourcenname, die Ressourcen-GUID oder die Element-GUID sein. Wenn Sie "?name=*Target Resource Name*" auslassen, wird Ressourcenmanager mit folgendem Fehler geöffnet:

  ```
  Keine Ressourcen-GUID angegeben.
  ```

  Wenn Sie eine Datenbank verwenden, in der die Groß- und Kleinschreibung beachtet wird, stellen Sie sicher, dass die Schreibweise der Zielressource der in der Configuration Management Database (CMDB) entspricht.

Anzeigen der Inventardaten für eine Datenklasse

Mit Ressourcenmanager können Sie Ereignisdaten für eine bestimmte Datenklasse anzeigen. Die angezeigten Inventardaten hängen von der gewählten Datenklasse ab. Im Allgemeinen können Sie Status- und aktuelle Daten anzeigen. Wenn verfügbar, werden auch Verlaufsdaten angezeigt.

Siehe "Zugreifen auf Ressourcenmanager" auf Seite 455.

So zeigen Sie Inventardaten für eine Datenklasse an

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Ressource".
2. Wählen Sie im Dialogfeld "Ressource auswählen" die Ressource aus, die Sie verwalten möchten, und klicken Sie dann auf "OK"
3. Klicken Sie im Ressourcenmanager im Menü "Ansicht" auf "Inventarisierung".
4. Wählen Sie in der Verzeichnisstruktur die Datenklasse aus, für die Sie Inventardaten anzeigen möchten.
5. Klicken Sie im rechten Teilfenster auf die Registerkarte, die die gewünschten Informationen enthält.

Anzeigen der Ereignisdaten für eine Datenklasse

Mit Ressourcenmanager können Sie Ereignisdaten für eine bestimmte Datenklasse anzeigen. Die angezeigten Ereignisdaten hängen von der gewählten Datenklasse ab. Im Allgemeinen können Sie Status- und aktuelle Daten der Datenklassenereignisse anzeigen.

So zeigen Sie Ereignisdaten für eine Datenklasse an

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Ressource".
2. Wählen Sie im Dialogfeld "Ressource auswählen" die Ressource aus, die Sie verwalten möchten, und klicken Sie dann auf "OK"
3. Klicken Sie im Ressourcenmanager im Menü "Ansicht" auf "Ereignisse".

   Siehe "Zugreifen auf Ressourcenmanager" auf Seite 455.
4. Wählen Sie in der Verzeichnisstruktur die Datenklasse aus, für die Sie Ereignisdaten anzeigen möchten.
5. Klicken Sie im rechten Teilfenster auf die Registerkarte, die die gewünschten Informationen enthält.

Hinzufügen einer Ressource zu einer Organisationsgruppe

Im Dialogfeld "Einer Organisationsgruppe hinzufügen " können Sie die ausgewählte Ressource einer Organisationsgruppe hinzufügen. Eine Ressource kann nur einmal in jeder Organisationsansicht vorkommen.

So fügen Sie eine Ressource einer Organisationsgruppe hinzu

1. Klicken Sie in der Symantec Management Console im Menü "Verwaltung" auf "Ressource".
2. Wählen Sie im Dialogfeld "Ressource auswählen" die Ressource aus, die Sie verwalten möchten, und klicken Sie dann auf "OK".
3. Klicken Sie im linken Teilfenster des Ressourcenmanagers auf den Link "Einer Organisationsgruppe hinzufügen".
4. Wählen Sie im Dialogfeld "Einer Organisationsgruppe hinzufügen" die Organisationsgruppe aus, der die Ressource hinzugefügt werden soll.
5. Klicken Sie auf "OK".

Siehe "Ressourcenmanager-Aufgaben" auf Seite 457.

Ressourcenmanager-Aufgaben

Mithilfe des Ressourcenmanagers können Sie eine Reihe von Aufgaben im Zusammenhang mit Ressourcen erledigen. Diese Aufgaben sind im Ressourcenmanager über das Menü "Aufgaben" verfügbar. Welche Aufgaben verfügbar sind, richtet sich nach dem Typ der ausgewählten Ressource.

Siehe "Informationen zur Ressourcenverwaltung" auf Seite 454.

Tabelle 27-1 Ressourcenmanager-Aufgaben

Aufgabe	Beschreibung
Auf das Aufgabenverwaltungs-portal zugreifen	Wenn die Aufgabe, die Sie durchführen möchten, nicht im linken Teilfenster aufgeführt ist, öffnen Sie das Aufgabenverwaltungsportal. Dort sind weitere Aufgaben verzeichnet.
Eine Ressource einer Organisations-gruppe hinzufügen	Sie können die ausgewählte Ressource einer Organisationsgruppe hinzufügen oder sie an eine neue Organisationsgruppe verschieben. Wenn Sie eine Organisationsgruppe innerhalb einer Organisationsansicht auswählen, der die Ressource noch nicht angehört, wird die Ressource dieser Gruppe hinzugefügt. Bei Auswahl einer Organisationsgruppe innerhalb einer Organisationsansicht, der die Ressource bereits angehört, wird die bisherige Organisationsgruppe durch die neue ersetzt.
Ressource löschen	Sie können die ausgewählte Ressource aus der Konfigurationsmanagement-Datenbank (CMDB) löschen.
Doppelte Unternehmens-ressourcen zusammenführen	(Nur Unternehmensressourcen) Wenn für ein Unternehmen zwei Einträge vorliegen, können Sie diese mit dieser Funktion zusammenführen.
Ping-Signal an Computer senden	Mit der Option "Computer anpingen" im Menü "Aufgabe" können Sie ein Ping-Signal an den ausgewählten Computer senden.
Aufgabe planen	Mit der Option "Aufgabe planen" im Menü "Aufgabe" können Sie die Ausführung eines Auftrags oder einer Aufgabe planen.
Organisations-übersicht anzeigen	Sie können ("Übersichten" > "Organisationsübersicht") die Organisationsgruppen anzeigen, zu denen die ausgewählte Ressource gehört.
Kalender anzeigen	Zeigen Sie Zeitplaninformationen von Notification Server über die Option "Kalender" im Menü "Ansicht" an. Siehe "Anzeigen des internen Zeitplankalenders des Notification Servers" auf Seite 130.
Ereignisse anzeigen	Sie können Ereignisdaten für eine Datenklasse, einschließlich allgemeiner Informationen über die Klasse und ihren Status einsehen. Siehe "Anzeigen der Ereignisdaten für eine Datenklasse" auf Seite 456.

Aufgabe	Beschreibung
Inventar anzeigen	Sie können Inventardaten für eine Datenklasse, einschließlich allgemeiner Informationen über die Klasse und ihren Status einsehen. Siehe "Anzeigen der Inventardaten für eine Datenklasse " auf Seite 456.
Ressourcen-zuordnungen anzeigen	Im linken Teilfenster können Sie die Ressourcen anzeigen, denen die ausgewählte Ressource zugeordnet ist. Wenn Sie die zugeordnete Ressource im linken Teilfenster auswählen, können Sie sie mit dem Ressourcenmanager verwalten.
Ressourcendetails anzeigen	Beim Öffnen des Ressourcenmanagers werden Details über die ausgewählte Ressource im rechten Teilfenster angezeigt.
Ressourcen-zuordnungen anzeigen	Über die Option "Ressourcenzuordnung" im Menü "Ansicht" können Sie Informationen über Ressourcenzuordnungen aufrufen. Auf der Seite "Ressourcenzuordnungen" werden Informationen über den Typ der Ressourcenzuordnung und die mit der ausgewählten Ressource assoziierten Namen von Ressourcentypen aufgeführt. Siehe "Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten" auf Seite 461.

Kapitel 28

Verwenden von Notification Server-Berichten

In diesem Kapitel werden folgende Themen behandelt:

- Infos zu Notification Server-Berichten
- Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten

Infos zu Notification Server-Berichten

Sie können Ihre Ressourcendaten mit Hilfe von Notification Server-Berichten anzeigen und verwalten. Diese Berichte enthalten Informationen über die verwalteten und nicht verwalteten Computer und die Notification Server-Konfiguration. Installierte Lösungen stellen daneben auch Berichte mit anwendungsspezifischen Informationen zur Verfügung. Diese Berichte geben beispielsweise Aufschluss darüber, welche Ereignisse und Automatisierungsrichtlinien Notification Server ausführt und wie lange diese dauern.

Berichte können so gestaltet werden, dass nur bestimmte Benutzer einen Bericht ausführen können. Ferner lassen sich Berichte einschränken, damit nur die Daten enthalten sind, auf die der Benutzer, der den Bericht ausführt, zugreifen darf. Beispiel: Wenn ein Manager einen Gehaltsbericht ausführt, sind nur Daten über das Gehalt der ihm unterstellten Mitarbeiter enthalten.

In den Berichten können Sie Informationen auf verschiedene Arten anzeigen. Sie können Ihre Informationen in Tabellen oder grafisch in Diagrammen anzeigen. Sie können sich auch auf bestimmte Objekte in einem Bericht konzentrieren, um zusätzliche Information zu beziehen.

Siehe "Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten" auf Seite 461.

Notification Server bietet eine große Auswahl an Berichten. Sie können diese Standardberichte zwar nicht ändern, aber Sie können sie duplizieren und die duplizierten Berichte dann entsprechend ihrer Anforderungen bearbeiten. Außerdem können Sie neue benutzerdefinierte Berichte erstellen.

Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten

Sie können Berichte verwenden, um Ressourcendaten anzuzeigen und zu verwalten. Berichte rufen Daten aus der CMDB ab.

Siehe "Infos zu Notification Server-Berichten" auf Seite 460.

Tabelle 28-1 Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten

Schritt	Aktion	Beschreibung
Schritt 1	Berichtergebnisse extrahieren.	Wählen Sie den gewünschten Bericht aus, legen Sie optional die Benutzerparameter fest und wählen Sie den zu verwendenden Snapshot aus. Siehe "Extrahieren von Notification Server-Berichtsergebnissen" auf Seite 462.
Schritt 2	Berichtergebnisse anzeigen.	Die Berichtanzeige kann wie folgt an Ihre Anforderungen angepasst werden: ■ Wählen Sie die Raster- oder Diagrammansicht aus, falls weitere Ansichten für den Bericht erstellt wurden. ■ Gruppieren und sortieren Sie die Spalten in der Rasteransicht. ■ Zeigen Sie die Ergebnisse in einer Diagrammansicht an (sofern die Diagrammansicht für den Bericht konfiguriert wurde). Siehe "Anzeigen von Notification Server-Berichtsergebnissen" auf Seite 464.

Schritt	Aktion	Beschreibung
Schritt 3	(Optional) Berichtergebnisse verwenden.	Sie können Berichtergebnisse folgendermaßen verwenden: ■ Um ausführliche Informationen zu erhalten, führen Sie einen Drilldown auf ausgewählte Objekte durch. Wenn Sie einen Drilldown für ein Element ausführen, wird die zugehörige Ansicht geöffnet. Bei dieser kann es sich um einen weiteren Bericht oder die Ressourcenmanager-Konsole handeln. ■ Führen Sie Aktionen auf ausgewählten Objekten durch. ■ Drucken Sie die Berichtergebnisse. Siehe "Verwenden der Notification Server-Berichtsergebnisse" auf Seite 465.
Schritt 4	(Optional) Berichtergebnisse speichern.	Sie können die Berichtergebnisse in den folgenden Formaten speichern: ■ Datei Arbeitsblatt (.csv), HTML- und XML-Dateitypen sind bei Notification Server inbegriffen. Installierte Lösungen bieten u. U. Optionen für weitere Dateitypen. Siehe "Speichern von Notification Server-Berichtsergebnissen als Datei" auf Seite 466. ■ Statischer Filter Siehe "Erstellen eines statischen Filters aus Notification Server-Berichtergebnissen" auf Seite 467. ■ Snapshot Siehe "Speichern von Notification Server-Berichtsergebnissen als Snapshot" auf Seite 468. ■ Web-Part Siehe "Speichern von Notification Server-Berichtsergebnissen als Web-Part" auf Seite 469.

Extrahieren von Notification Server-Berichtsergebnissen

Im Lieferumfang von Notification Server ist eine Reihe von Berichten enthalten. Installierte Lösungen enthalten ggf. weitere Berichte.

Manche Berichte enthalten Benutzerparameter, die Sie beim Extrahieren der Berichtsergebnisse festlegen können. Benutzerparameter sind Variablen in der Berichtsabfrage, mit denen die Berichte flexibler und aussagekräftiger gestaltet werden können. Beispielsweise besitzt der Bericht über die Computerliste Benutzerparameter, die sowohl für den Systemtyp als auch das Betriebssystem definiert sind. Beim Extrahieren von Berichtsergebnissen können Sie die gewünschte Kombination aus Systemtyp und Betriebssystem angeben, indem Sie die

entsprechenden Parameter einstellen. Ohne Benutzerparameter würde jeder Bericht über feste in der Abfrage festgelegte Werte verfügen. Sie benötigen dann einen anderen Bericht für jede Systemstyp- und Betriebssystemkombination. Sie können auch die Berichtsabfrage jedesmal ändern, wenn Sie Ergebnisse extrahieren möchten.

Um die Belastung für Notification Server zu minimieren, werden große oder häufig ausgeführte Berichte üblicherweise zu einem geeigneten Zeitpunkt erstellt und als Snapshot gespeichert. Mit Hilfe von Snapshots können alle anderen Benutzer die Berichtergebnisse im neuesten Schnappschuss einsehen, anstatt dass jeder Benutzer den Bericht erneut ausführt. Die geplanten Berichte werden in der Regel mit Administratorrechten ausgeführt, um sicherzustellen, dass alle verfügbaren Daten enthalten sind. Beim Anzeigen der Berichtergebnisse werden die Daten des Snapshots dementsprechend berücksichtigt. Wenn Sie Berichtergebnisse anzeigen, können Sie einen Snapshot auswählen. Wird kein Snapshot ausgewählt, werden die Ergebnisse durch Ausführen der Berichtsabfrage in der CMDB abgerufen.

Für große Umgebungen empfiehlt Symantec die Funktion "SuppressReportAutorun". Ist "SuppressReportAutorun" aktiviert und Sie öffnen einen beliebigen Bericht, wird der Bericht nicht sofort ausgeführt. Damit die Ergebnisse des Berichts angezeigt werden, müssen Sie auf "Aktualisieren" klicken. Beachten Sie, dass die Funktion "SuppressReportAutorun" standardmäßig deaktiviert ist. Sie können sie in "NS-Konfigurator" unter "Core-Einstellungen > Benutzeroberfläche > Bericht > SuppressReportAutorun" aktivieren.

Siehe "Konfigurieren von Notification Server-Einstellungen mit NS Configurator" auf Seite 77.

Diese Aufgabe ist ein Schritt beim Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten.

Siehe "Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten" auf Seite 461.

So extrahieren Sie Notification Server-Berichtsergebnisse

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Wählen Sie im linken Teilfenster den gewünschten Bericht aus.
3. (Optional) Legen Sie im rechten Teilfenster unter "Parameter", die entsprechenden Benutzerparameter fest.

   Siehe "Definieren von Parametern und Value Providers für einen benutzerdefinierten Bericht" auf Seite 481.
4. Wenn Sie einen Snapshot verwenden möchten, wählen Sie diesen in der Dropdown-Liste "Ansicht" aus.

Folgende Optionen stehen zur Auswahl:

- Aktuell
- Neuester Snapshot

Alle weiteren von Ihnen erstellten Snapshots werden aufgelistet. Für jeden Schnappschuss sind Datum und Uhrzeit der Erstellung vermerkt.

Anzeigen von Notification Server-Berichtsergebnissen

Sie können die Berichtsergebnisse mithilfe folgender Ansichten anzeigen, wenn diese für den Bericht konfiguriert wurden:

Rasteransicht	Rasteransichten sind Tabellen, bei denen jedes Ergebnis in einer eigenen Zeile steht. Die verfügbaren Spalten werden im Bericht genannt. Sie können die Reihenfolge der Spalten ändern und die Ergebnisse entsprechend den Werten in einer bestimmten Spalte anordnen. Beispielsweise können Sie die Computer nach Betriebssystem oder Subnetz anzeigen.
Diagrammansicht	Diagrammansichten illustrieren die Daten in Form von Balken-, Linien-, Kreis- und Bereichsdiagrammen. In einem Bericht können mehrere Diagrammansichten definiert werden, Sie können aber immer nur eine Ansicht anzeigen.

Jedes Diagramm oder Raster gibt einen bestimmten Einblick in die Berichtergebnisse. Folglich kann eine Ansicht eine Teilmenge der Ergebnisse enthalten. Für einen Bericht können mehrere Ansichten vorliegen, mit denen sich die Ausgabe des Berichts an die Anforderungen verschiedener Benutzer anpassen lässt, anstelle dass für die einzelnen Benutzer verschiedene Berichte erstellt werden. Ein Bericht über verwaltete Computer enthält zum Beispiel die Eigenschaften der einzelnen Computer wie Betriebssystem, Prozessortyp und Datenträgergröße. Der Bericht kann über etliche verschiedene Ansichten verfügen, von denen jede eine Teilmenge der verfügbaren Eigenschaften der einzelnen Computer enthält. Wenn Sie den Bericht anzeigen, können Sie die Ansicht auswählen, in der die für Sie interessanten Eigenschaften aufgeführt werden.

Wenn Sie einen Bericht speichern, speichern Sie alle Ergebnisse, auf die Sie zugreifen dürfen. Ihr Zugriff wird nicht auf die soeben angezeigten Daten beschränkt. Wird ein Bericht gedruckt, so wird die aktuelle Ansicht gedruckt.

Diese Aufgabe ist ein Schritt beim Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten.

Siehe "Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten" auf Seite 461.

So zeigen Sie Notification Server-Berichtsergebnisse an

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Wählen Sie im linken Teilfenster den gewünschten Bericht aus.
3. Wählen Sie im rechten Teilfenster in der Dropdown-Liste "Ansicht" die gewünschte Ansicht aus.

   Die erstellten Raster- und Diagrammansichten werden aufgeführt.
4. (Optional) Wenn Sie die Ergebnisse gruppieren möchten, wählen Sie in der Dropdown-Liste "Gruppieren nach" die gewünschte Spalte aus.
5. (Optional) Sie können die Reihenfolge der Spalten ändern, indem Sie auf eine Spaltenüberschrift klicken und die Spalte an die gewünschte Stelle ziehen.

Verwenden der Notification Server-Berichtsergebnisse

Sie können einen Drilldown für Berichtergebnisse durchführen, um zusätzliche Informationen zu erhalten. Wenn Sie einen Drilldown für ein Element ausführen, wird die zugehörige Ansicht geöffnet. Bei dieser kann es sich um einen weiteren Bericht oder den Ressourcenmanager handeln.

Sie können Aktionen für Ressourcen direkt von den Berichtergebnissen durchführen. Beispielsweise können Sie einen Bericht ausführen, der alle Computer auflistet, die bestimmte Kriterien erfüllen. Sie können anschließend eine Aktion für einige oder alle Computer durchführen. Zu den verfügbaren Aktionen gehören diejenigen, die für den ausgewählten Ressourcentyp gelten, und für die Sie eine Berechtigung zur Durchführung haben.

Sie können ausgewählte Zeilen von Ergebnissen oder alle Berichtergebnisse drucken.

Diese Aufgabe ist ein Schritt beim Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten.

Siehe "Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten" auf Seite 461.

So führen Sie einen Drilldown für Berichtergebnisse durch

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Wählen Sie im linken Teilfenster den gewünschten Bericht aus.

3 Wählen Sie im rechten Teilfenster in der Dropdown-Liste "Ansicht" die gewünschte Ansicht aus.

4 Klicken Sie in den Berichtergebnissen auf das Element, für das Sie zusätzliche Informationen möchten.

Beachten Sie, dass die Drilldown-Aktion unterschiedlich sein kann: Es kann sich dabei um einen einzelnen oder einen Doppelklick handeln.

So führen Sie Aktionen für in den Berichtergebnissen aufgelistete Ressourcen durch

1 Wählen Sie in den Berichtergebnissen die Ressourcen aus, für die Sie eine Aktion durchführen möchten.

2 Klicken Sie auf "Aktionen", und wählen Sie anschließend die entsprechende Option aus.

Beachten Sie, dass diese Funktion nicht immer verfügbar ist.

So drucken Sie Berichtergebnisse

1 Wählen Sie bei Bedarf in den Berichtergebnissen die Zeilen der Berichtergebnisse aus, die Sie drucken möchten.

2 Klicken Sie auf "Drucken".

3 Geben Sie im Dialogfeld "Drucken" die folgenden Einstellungen an:

Parameter	Wenn die Einstellungen mit den Benutzerparametern in den gedruckten Ergebnissen enthalten sein sollen, aktivieren Sie "Parameter einschließen".
Datenbereich	Wählen Sie eine der folgenden Optionen aus: ■ Alle drucken - Enthält alle Berichtergebnisse. ■ Ausgewählte Zeilen drucken - Enthält nur die ausgewählten Zeilen von Berichtergebnissen.

4 Klicken Sie auf "Drucken".

Eine Vorschau des Berichtausdrucks wird in einem neuen Browserfenster gezeigt und das Dialogfeld "Windows - Drucken" wird angezeigt. Die Vorschau ist mit derjenigen beim Speichern des Berichts als HTML-Datei identisch.

5 Wählen Sie im Dialogfeld "Windows - Drucken" die entsprechenden Optionen aus, und klicken Sie anschließend auf "Drucken".

Speichern von Notification Server-Berichtsergebnissen als Datei

Sie können die Berichtergebnisse als Datei speichern. Sie können alle Ergebnisse speichern oder die Ergebnisse auswählen, die enthalten sein sollen. Optionen für

Tabellenkalkulations- (.csv), HTML- und XML-Dateitypen werden durch Notification Server bereitgestellt. Installierte Lösungen können Optionen für zusätzliche Dateitypen zur Verfügung stellen.

Diese Aufgabe ist ein Schritt beim Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten.

Siehe "Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten" auf Seite 461.

So speichern Sie Notification Server-Berichtergebnisse als Datei

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Wählen Sie im linken Teilfenster den gewünschten Bericht aus.
3. (Optional) Wählen Sie im rechten Teilfenster die Berichtsergebniszeilen aus, die in der Datei enthalten sein sollen.
4. Klicken Sie auf "Speichern unter", und klicken Sie dann auf den entsprechenden Dateityp.
5. Geben Sie im Dialogfeld "Speichern unter" die folgenden Einstellungen an:

Parameter	Wenn die Einstellungen mit den Benutzerparametern in der Datei enthalten sein sollen, aktivieren Sie "Parameter einschließen".
Datenbereich	Wählen Sie eine der folgenden Optionen aus: ■ "Alles Speichern" - Schliesst alle Berichtergebnisse im Filter ein. ■ "Ausgewählte Zeilen speichern" - Schliesst nur die ausgewählten Zeilen der Berichtergebnisse im Filter ein.

6. Klicken Sie auf "Speichern".
7. Wählen Sie im Dialogfeld "Bericht speichern" den Ordner aus, in dem die Datei gespeichert werden soll, und klicken Sie anschließend auf "Speichern".

Erstellen eines statischen Filters aus Notification Server-Berichtergebnissen

Sie können einen neuen statischen Filter erstellen, indem Sie die Ergebnisse eines Berichts speichern. Sie können alle Ergebnisse einbeziehen oder die Ergebnisse auswählen, die enthalten sein sollen.

Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Diese Aufgabe ist ein Schritt beim Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten.

Siehe "Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten" auf Seite 461.

So erstellen Sie einen statischen Filter aus Notification Server-Berichtergebnissen

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Wählen Sie im linken Teilfenster den gewünschten Bericht aus.
3. (Optional) Wählen Sie im rechten Teilfenster die Berichtsergebniszeilen aus, die im Filter enthalten sein sollen.
4. Klicken Sie auf "Speichern unter" > "Statischer Filter".
5. Geben Sie im Dialogfeld "Als statischen Filter speichern" die entsprechenden Einstellungen an:

Name	Standardeinstellung ist der Berichtname. Wenn Sie den Namen ändern möchten, geben Sie den entsprechenden Filternamen ein.
Ressource als Basis für den Filter auswählen	Diese Option gilt nur für Ressourcenberichte. Wählen Sie in der Dropdown-Liste die entsprechende Option aus.
Datenbereich	Wählen Sie eine der folgenden Optionen aus: ■ "Alles Speichern" - Schliesst alle Berichtergebnisse im Filter ein. ■ "Ausgewählte Zeilen speichern" - Schliesst nur die ausgewählten Zeilen der Berichtergebnisse im Filter ein.

6. Klicken Sie auf "Speichern".

   Der neue Filter wird in der Struktur "Filter" im Ordner "Berichtsbasierte Filter" gespeichert.

Speichern von Notification Server-Berichtsergebnissen als Snapshot

Sie können die aktuellen Berichtergebnisse als Snapshot speichern. Beispielsweise empfiehlt es sich, bestimmte Ergebnisse zu speichern und sie anderen Benutzern zugänglich zu machen, ohne sie wieder aus der CMDB zu extrahieren. Wenn Sie einen Bericht als Snapshot speichern, wird er entsprechend Ihrem Bereich

gespeichert. Nur Benutzer, die die gleiche Sicherheitsrolle haben, können den Snapshot anzeigen.

Diese Aufgabe ist ein Schritt beim Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten.

Siehe "Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten" auf Seite 461.

So speichern Sie Notification Server-Berichtergebnisse als Snapshot

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Wählen Sie im linken Teilfenster den gewünschten Bericht aus.
3. Klicken Sie im rechten Teilfenster auf "Speichern unter" > "Snapshot".

   Wenn Sie den Bericht das nächstes Mal öffnen, ist der neue Snapshot in der Dropdown-Liste "Ansicht" verfügbar.

Speichern von Notification Server-Berichtsergebnissen als Web-Part

Sie können einen Bericht als Web-Part speichern, den Sie auf einer Portalseite verwenden können. Der Web-Part-Bericht ist eine Kopie des Berichts, der dynamisch und voll funktionsfähig ist. Das in der Portalseite angezeigte Ergebnis wird beim Öffnen der Seite aktualisiert, so dass es immer aktuell ist. Der Web-Part-Bericht ist unabhängig vom ursprünglichen Bericht, so dass Änderungen an einem Bericht nicht an den anderen Bericht weitergeleitet werden.

Siehe "Erstellen und Ändern von Web-Parts" auf Seite 62.

Diese Aufgabe ist ein Schritt beim Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten.

Siehe "Anzeigen und Verwalten von Ressourcendaten mit Notification Server-Berichten" auf Seite 461.

So speichern Sie Notification Server-Berichtsergebnisse als Web-Part

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Wählen Sie im linken Teilfenster den gewünschten Bericht aus.
3. Klicken Sie im rechten Teilfenster auf "Speichern unter" > "Web-Part".
4. (Optional) Bearbeiten Sie im Dialgfeld "Als Web-Part speichern" den Namen des neuen Web-Parts.

   Der Standardname sollte für die meisten Zwecke geeignet sein.

5 (Optional) Wählen Sie in der Dropdown-Liste "Web-Part-Größe auswählen" die passende Größe aus.

Die Standardeinstellung ist "Klein".

6 Klicken Sie auf "Speichern".

Der neue Web-Part wird im Ordner "Settings\Console Settings\Webparts" gespeichert.

Kapitel 29

Erstellen benutzerdefinierter Notification Server-Berichte

In diesem Kapitel werden folgende Themen behandelt:

- Komponenten eines benutzerdefinierten Notification Server-Berichts
- Erstellen und Ändern benutzerdefinierter Notification Server-Berichte

Komponenten eines benutzerdefinierten Notification Server-Berichts

Notification Server-Berichte beruhen auf einer Reihe von Standardkomponenten.

Tabelle 29-1 Die Komponenten eines benutzerdefinierten Notification Server-Berichts

Komponente	Beschreibung
Datenquelle	Die Datenquelle ist die Komponente, die die Berichtdaten liefert. Benutzerdefinierte Berichte und dynamische Filter nutzen SQL-Abfragen, die auf der CMDB ausgeführt werden, um die entsprechenden Daten zu extrahieren. Lösungen können Berichte generieren, die andere Datenquellen (z.B. Kalkulationstabellen oder CSV-Dateien) verwenden. Benutzerdefinierte Berichte und dynamische Filter verwenden eine SQL-Abfrage als Datenquelle. Sie können die Abfrage definieren, indem Sie das SQL neu schreiben oder mithilfe des Abfragegenerators erstellen. Siehe "Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht" auf Seite 478. Siehe "Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht" auf Seite 480.
Ansichten	Die Berichtansicht ist die Art und Weise, wie Berichtdaten angezeigt werden. Eine Ansicht enthält gewöhnlich eine Teilmenge der Berichtsdaten. Die Daten werden auf eine Weise dargestellt, die einer bestimmten Benutzerrolle entspricht. Sie können die in der Ansicht angezeigten Datenspalten auswählen und angeben, welche als primäre Achse verwendet werden soll. Es gibt folgende Typen von Ansichten: ■ Rasteransicht Die Berichtdaten werden in einer Tabelle in einzelnen Zeilen abgebildet. ■ Diagrammansicht Die Berichtdaten werden als Grafik abgebildet, d. h. in Form von Balken-, Linien-, Kreis- und Bereichsdiagrammen. ■ Vorlagentext Wenn Sie verschiedene Ansichten für einen Bericht festlegen, können Sie die Berichtdaten auf unterschiedliche Benutzer zuschneiden. So können Sie einen einzigen Bericht für alle Benutzer verwenden anstatt mehrere Berichte für spezifische Benutzeranforderungen zu erstellen. Siehe "Erstellen oder Ändern einer Diagrammansicht für einen benutzerdefinierten Bericht" auf Seite 483. Siehe "Erstellen oder Ändern einer Rasteransicht für einen benutzerdefinierten Bericht" auf Seite 485.

Komponente	Beschreibung
Parameter	Parameter sind Variablen in der Berichtabfrage, die der Benutzer beim Ausführen des Berichts einstellen kann. Mithilfe von Parametern lassen sich Berichte flexibel gestalten. Beispielsweise enthält der Bericht "Computerliste nach Systemtyp und OS-Name" die sowohl für den Systemtyp als auch das Betriebssystem definierten Parameter. Wird dieser Bericht nun ausgeführt, können Sie die gewünschte Kombination aus Systemtyp und Betriebssystem durch Festlegung der jeweiligen Parameter angeben. Ohne Parameter würde jeder Bericht über feste, in der Abfrage definierte Werte verfügen. Siehe "Definieren von Parametern und Value Providers für einen benutzerdefinierten Bericht" auf Seite 481.
Drilldowns	Ein Bericht-Drilldown ist eine Aktion, die durchgeführt wird, wenn der Benutzer auf ein Element in den Berichtergebnissen klickt. Es empfiehlt sich, Berichte mit Drilldowns zu versehen, damit der Benutzer anhand der Berichtergebnisse zusätzliche Informationen einholen kann. Für jeden Drilldown können Sie die Ansicht bestimmen, auf der der Drilldown verfügbar ist, und auch angeben, wie der Benutzer den Drilldown auslöst. Sie können auch die Aktion, die durchgeführt wird, und die für die Aktion verwendeten Parameter festlegen. Um verschiedene Aktionen für verschiedene Ressourcentypen durchzuführen, können Sie in einem Bericht mehrere Drilldowns einrichten. Siehe "Einrichten der Drilldown-Aktionen für einen benutzerdefinierten Bericht" auf Seite 486.

Erstellen und Ändern benutzerdefinierter Notification Server-Berichte

Anhand von Notification Server-Berichten können Sie Ihre Ressourcendaten anzeigen und verwalten. Diese Berichte enthalten Informationen über Ihre verwalteten und nicht verwalteten Computer sowie Ihre Notification Server-Konfiguration. Eine große Auswahl von Berichten wird mit Symantec Management-Plattform bereitgestellt. Sie können auch Ihre eigenen benutzerdefinierten Berichte den Anforderungen Ihrer Organisation entsprechend erstellen. Notification Server-Berichte rufen Daten von der Configuration Management Database (CMDB) ab.

Die Berichtsdaten können folgendermaßen verwendet werden:

- Datenquelle für eine Automatisierungsrichtlinie

- Web-Part, das aktuelle Daten auf einer Portalseite anzeigt
- Ressourcenbericht, anhand dessen der Benutzer einen Drilldown für eine bestimmte Ressource durchführt, um komplette Details im Ressourcenmanager anzuzeigen
- Trendbericht, der Datenänderungen im Lauf der Zeit anzeigt
- Mehrere Drilldown-Berichte (z. B. Hierarchieberichte), anhand derer der Benutzer einen Drilldown für Daten auf hoher Ebene durchführt, um detailliertere Daten auf niedriger Ebene anzuzeigen.

Um einen benutzerdefinierten Bericht zu erstellen oder zu ändern, müssen Sie die Komponenten des Berichts auf der Seite "Benutzerdefinierte Berichte bearbeiten" definieren.

Siehe "Seite "Benutzerdefinierte Berichte bearbeiten"" auf Seite 549.

Siehe "Komponenten eines benutzerdefinierten Notification Server-Berichts" auf Seite 471.

Hinweis: In einigen Automatisierungsrichtlinien werden Berichte als Datenquelle genutzt. Daneben können die Richtlinien von bestimmten Ergebnissen oder Parametern abhängen. Stellen Sie beim Ändern von Berichten sicher, dass sich die Änderungen nicht auf eine Automatisierungsrichtlinie auswirken.

Siehe "Angeben der Datenquelle für Automatisierungsrichtlinien" auf Seite 419.

Tabelle 29-2 Verfahren zum Erstellen und Ändern benutzerdefinierter Notification Server-Berichte

Schritt	Aktion	Beschreibung
Schritt 1	Erstellen Sie einen neuen Bericht, oder wählen Sie einen vorhandenen Bericht zum Ändern aus.	Erstellen Sie den neuen Bericht von Grund auf neu, oder kopieren Sie einen von Notification Server bereitgestellten Standardbericht. Sämtliche von Ihnen erstellte Berichte können geändert werden. Die Standardberichte dagegen nicht. Siehe "Erstellen eines benutzerdefinierten Notification Server-Berichts" auf Seite 476. Siehe "Ändern eines vorhandenen benutzerdefinierten Notification Server-Berichts" auf Seite 478.

Schritt	Aktion	Beschreibung
Schritt 2	Erstellen Sie die Berichtabfrage.	Um die Berichtabfrage zu erstellen, schreiben Sie das Abfrage-SQL entweder selbst oder verwenden Sie den Abfragegenerator. Mit dem benutzerfreundlichen Abfragegenerator können Sie die Tabellen und Felder auswählen, die Sie verwenden möchten. Siehe "Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht" auf Seite 478. Sie können den SQL-Code von Grund auf schreiben. Alternativ können Sie SQL aus einem anderen Filter oder Bericht kopieren und Ihren Anforderungen entsprechend ändern. Siehe "Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht" auf Seite 480.
Schritt 3	Geben Sie an, woher die Parameter ihre Werte erhalten.	Wenn die Berichtabfrage Parameter enthält, können Sie den entsprechenden Wertanbieter festlegen. Mithilfe des Wertanbieters können Benutzer beim Ausführen der Abfrage den geeigneten Wert für den Abfrageparameter einstellen. Siehe "Definieren von Parametern und Value Providers für einen benutzerdefinierten Bericht" auf Seite 481.
Schritt 4	Erstellen Sie die Berichtansichten.	Eine Berichtsansicht enthält gewöhnlich eine Teilmenge der Berichtergebnisse. Die Ergebnisse werden auf eine Weise dargestellt, die einer bestimmten Benutzerrolle entspricht. Wenn Sie verschiedene Ansichten für einen Bericht festlegen, können Sie die Berichtergebnisse auf unterschiedliche Benutzer zuschneiden. Siehe "Erstellen oder Ändern einer Diagrammansicht für einen benutzerdefinierten Bericht" auf Seite 483. Siehe "Erstellen oder Ändern einer Rasteransicht für einen benutzerdefinierten Bericht" auf Seite 485.
Schritt 5	Erstellen Sie Drilldowns.	Ein Bericht-Drilldown ist eine Aktion, die durchgeführt wird, wenn der Benutzer auf ein Element in den Berichtergebnissen klickt. Es empfiehlt sich, Drilldowns für einen Bericht zu konfigurieren, damit der Benutzer anhand der Berichtergebnisse zusätzliche Informationen einholen kann. Siehe "Einrichten der Drilldown-Aktionen für einen benutzerdefinierten Bericht" auf Seite 486.

Schritt	Aktion	Beschreibung
Schritt 6	Geben Sie die Berichteigenschaften an.	Sie können auswählen, ob die Berichtergebnisse auf den Bereich des Benutzers eingeschränkt werden, der den Bericht ausführt. Sie können auch auswählen, den Bericht nur als Snapshot auszuführen. Um die Belastung des Notification Servers zu minimieren, können Sie große oder häufig verwendete Berichte als Snapshots ausführen. Siehe "Festlegen der erweiterten Eigenschaften eines benutzerdefinierten Berichts" auf Seite 489.
Schritt 7	Speichern Sie den Bericht.	Speichern Sie den neuen oder geänderten Bericht. Siehe "Erstellen eines benutzerdefinierten Notification Server-Berichts" auf Seite 476. Siehe "Ändern eines vorhandenen benutzerdefinierten Notification Server-Berichts" auf Seite 478.

Erstellen eines benutzerdefinierten Notification Server-Berichts

Sie können Ihre eigenen benutzerdefinierten Berichte erstellen und konfigurieren, um Ihren Anforderungen zu entsprechen. Sie können einen vollständig neuen Bericht erstellen oder einen Standardbericht duplizieren, der mit Notification Server geliefert wird.

Diese Aufgabe ist ein Schritt beim Erstellen und Ändern von Notification Server-Berichten.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

So erstellen Sie einen benutzerdefinierten Notification Server-Bericht

1. Wählen Sie in der Symantec Management Console im Menü "Berichte" die Option "Alle Berichte".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, dem Sie den neuen Bericht hinzufügen möchten, und klicken Sie dann auf "Neu > Bericht".

3 Klicken Sie auf eine der folgenden Optionen:

Computerbericht	Die Berichtsabfrage ist eine Ressourcenabfrage und mit der Basisvorlage werden alle Computer ausgewählt. Sie können die Abfrage verfeinern, um alle gewünschten Computer auszuwählen.
Benutzerbericht	Die Berichtsabfrage ist eine Ressourcenabfrage und mit der Basisvorlage werden alle Benutzer ausgewählt. Sie können die Abfrage verfeinern, um alle gewünschten Benutzer auszuwählen.
Ressourcenbericht	Die Berichtsabfrage ist eine Ressourcenabfrage und mit der Basisvorlage werden alle Ressourcen (einschließlich aller Computer und Benutzer) ausgewählt. Sie können die Abfrage verfeinern, um alle gewünschten Ressourcen auszuwählen.
SQL-Bericht	Die Berichtsabfrage ist eine SQL-Abfrage. Sie können Ihre eigene SQL-Abfrage schreiben, um die gewünschten Daten aus der CMDB abzurufen. Es wird keine Vorlage verwendet und es gibt keine Einschränkungen für das, was Sie schreiben.

4 (Optional) Geben Sie im rechten Teilfenster den Berichtnamen und die Beschreibung an.

5 Geben Sie auf der Seite "Benutzerdefinierte Berichte bearbeiten" die Berichtskomponenten und -eigenschaften auf den entsprechenden Registerkarten an.

Siehe "Seite "Benutzerdefinierte Berichte bearbeiten"" auf Seite 549.

Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.

6 Um die Änderungen zu speichern ohne den Bearbeitungsmodus zu verlassen, klicken Sie auf "Übernehmen".

7 Um eine Vorschau der Änderungen anzuzeigen ohne den Bearbeitungsmodus zu verlassen, klicken Sie auf "Vorschau".

8 Um die Änderungen zu speichern und den Bearbeitungsmodus zu beenden, klicken Sie auf "Änderungen speichern".

Ändern eines vorhandenen benutzerdefinierten Notification Server-Berichts

Sie können Ihre eigenen benutzerdefinierten Berichte jederzeit ändern. Sie können die Standardberichte nicht ändern, die mit Notification Server ausgeliefert werden. Wenn Sie einen Standardbericht ändern möchten, können Sie den Bericht duplizieren, um eine Kopie davon zu erstellen und diese dann zu bearbeiten.

Diese Aufgabe ist ein Schritt beim Erstellen und Ändern von Notification Server-Berichten.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

So ändern Sie einen vorhandenen benutzerdefinierten Notification Server-Bericht

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Klicken Sie im linken Bereich auf den Bericht, den Sie bearbeiten möchten.
3. Klicken Sie im rechten Teilfenster in der rechten oberen Ecke auf "Bearbeiten".
4. (Optional) Ändern Sie den Berichtnamen und die Beschreibung.
5. Nehmen Sie auf der Seite "Benutzerdefinierte Berichte bearbeiten" Ihre Änderungen an den Berichtkomponenten und Berichteigenschaften auf den entsprechenden Registerkarten vor.

   Siehe "Seite "Benutzerdefinierte Berichte bearbeiten"" auf Seite 549.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.
6. Um die Änderungen zu speichern ohne den Bearbeitungsmodus zu verlassen, klicken Sie auf "Übernehmen".
7. Um eine Vorschau der Änderungen anzuzeigen ohne den Bearbeitungsmodus zu verlassen, klicken Sie auf "Vorschau".
8. Um die Änderungen zu speichern und den Bearbeitungsmodus zu verlassen, klicken Sie auf "Änderungen speichern".

Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht

Wenn Sie Ihren eigenen benutzerdefinierten Notification Server-Bericht erstellen oder ändern, können Sie eine Berichtsabfrage definieren. Für einen Computerbericht, Benutzerbericht oder Ressourcenbericht müssen Sie eine Ressourcenabfrage definieren.

Eine Ressourcenabfrage basiert auf den Tabellen, die in der Configuration Management Database (CMDB) verfügbar sind. Der Abfragegenerator ist ein benutzerfreundliches Tool, das eine Standardvorlage zur Verfügung stellt und die Auswahl gewünschter Tabellen und Felder erlaubt. Mit ihm können Sie die Abfrage wunschgemäß definieren. Dabei sind keine SQL-Kenntnisse erforderlich. Die Ressourcenabfrage wird automatisch in SQL konvertiert. Dieser Code wird dann in der CMDB ausgeführt, um die entsprechenden Ressourcen zu extrahieren.

Wenn Sie eine Ressourcenabfrage für einen benutzerdefinierten Bericht definiert haben, können Sie sie in die entsprechende SQL-Abfrage konvertieren. Beispiel: Sie können den Abfragegenerator verwenden, um die Struktur Ihrer Abfrage zu definieren, sie in SQL konvertieren und dann das SQL direkt ändern. Dies kann schneller und effizienter sein als die gesamte Abfrage in SQL von Grund auf neu zu schreiben.

Wenn Sie einen neuen Computer-, Benutzer- oder Ressourcenbericht erstellen, wird dem Bericht automatisch eine Ressourcenabfragevorlage hinzugefügt. Im Abfragemodus "Abfragegenerator" wird beim Erstellen eines neuen Filters dieselbe Ressourcenabfragevorlage dem Filter hinzugefügt. Mithilfe der in der Vorlage enthaltenen grundlegenden Abfrage werden alle Computer, Benutzer oder Ressourcen ausgewählt, die dem Berichttyp entsprechen. Um geeignete Ressourcen auszuwählen, ändern Sie die grundlegende Abfrage.

Diese Aufgabe ist ein Schritt beim Erstellen und Ändern von Notification Server-Berichten.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

So definieren Sie eine Ressourcenabfrage für einen benutzerdefinierten Bericht

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Sie haben folgende Möglichkeiten:
   - Um eine Ressourcenabfrage für einen neuen Bericht zu definieren, klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, der dem neuen Bericht hinzugefügt werden soll. Klicken Sie dann auf "Neu" und auf "Computerbericht", "Benutzerbericht" oder "Ressourcenbericht".
   - Um eine Ressourcenabfrage für einen vorhandenen Bericht umzudefinieren, klicken Sie im linken Teilfenster auf den gewünschten Computer-, Benutzer- oder Ressourcenbericht. Klicken Sie im rechten Fensterteil in der rechten oberen Ecke mit der rechten Maustaste auf "Bearbeiten".

3 Geben Sie im rechten Teilfenster auf der Registerkarte "Datenquelle" die Abfragedetails an.

Siehe "Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle" " auf Seite 550.

Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann F1 drücken.

4 (Optional) Klicken Sie zum Konvertieren der Ressourcenabfrage in eine gleichwertige SQL-Abfrage auf "Diese Abfrage in eine SQL-Abfrage konvertieren".

Warnung: Eine RessourcenAbfrage in eine SQL-Abfrage zu konvertieren ist eine "Einbahnstraße". Das heißt, eine Rückverwandlung der resultierenden SQL-Abfrage in die Ressourcen-Abfrage ist nicht möglich.

---

5 Klicken Sie auf "Änderungen speichern".

Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht

Wenn Sie Ihren eigenen benutzerdefinierten Notification Server-Bericht erstellen oder ändern, können Sie eine Berichtsabfrage definieren. Für einen Computerbericht, Benutzerbericht oder Ressourcenbericht müssen Sie eine Ressourcenabfrage definieren. Für einen SQL-Bericht müssen Sie eine SQL-Abfrage definieren.

Sie können eine SQL-Abfrage schreiben, um die Ressourcen zu definieren, die Sie im Bericht oder im Filter berücksichtigen möchten. Sie können den SQL-Code von Grund auf schreiben. Alternativ können Sie SQL aus einem anderen Filter oder Bericht kopieren und Ihren Anforderungen entsprechend ändern. Beispielsweise können Sie eine Ressourcenabfrage mit dem Abfragegenerator erstellen und anschließend das generierte SQL aus der Registerkarte "Abfrageauflösung" kopieren. Sie können auch den Abfragegenerator verwenden, um die Struktur Ihrer Abfrage zu definieren, sie in SQL zu konvertieren und dann das SQL direkt zu ändern.

Wenn Sie einen neuen SQL-Bericht erstellen, wird dem Bericht automatisch eine SQL-Abfragevorlage hinzugefügt. Beim Erstellen eines neuen Filters wird diesem die gleiche Ressourcenabfragevorlage hinzugefügt, wenn Sie den Abfragegenerator-Abfragemodus wählen. Die Basis-SQL-Abfrage wählt alle verfügbaren Ressourcen aus. Sie müssen die Basisabfrage ändern, um die passenden Ressourcen auszuwählen.

Sie benötigen die Berechtigung zum Bearbeiten von SQL, um SQL-Abfragen zu erstellen oder zu ändern. Zudem sollten Sie sich mit der CMDB-Tabellenstruktur

auskennen. Sollen Bereiche auf die Abfrageergebnisse angewendet werden, müssen Sie den entsprechenden SQL-Code in die Abfrage einfügen.

Diese Aufgabe ist ein Schritt beim Erstellen und Ändern von Notification Server-Berichten.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

So definieren Sie eine SQL-Abfrage für einen benutzerdefinierten Bericht

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Sie haben folgende Möglichkeiten:
   - Um eine SQL-Abfrage für einen neuen Bericht zu definieren, klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, der dem neuen Bericht hinzugefügt werden soll. Klicken Sie dann auf "Neu" und auf "SQL-Bericht".
   - Um eine SQL-Abfrage für einen vorhandenen Bericht umzudefinieren, klicken Sie im linken Teilfenster auf den SQL-Bericht, den Sie ändern möchten. Klicken Sie im rechten Fensterteil in der rechten oberen Ecke mit der rechten Maustaste auf "Bearbeiten".
3. Geben Sie im rechten Fensterteil auf der Registerkarte "Datenquelle" die Abfragedetails auf den entsprechenden Registerkarten an.

   Siehe "Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle" " auf Seite 550.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.
4. Klicken Sie auf "Änderungen speichern".

Definieren von Parametern und Value Providers für einen benutzerdefinierten Bericht

Wenn die Abfrage des benutzerdefinierten Berichts Parameter enthält, können Sie die entsprechenden Value Provider definieren. Anhand des Value Providers eines Parameters kann der Benutzer bei Ausführung des Berichts den entsprechenden Wert für den Parameter festlegen. Durch Einbeziehen benutzerdefinierbarer Parameter in einer Berichtsabfrage können Sie einen flexiblen Bericht erstellen, aus dem verschiedene Ergebnissätze durch Ändern der Parameterwerte extrahiert werden können. Die Alternative wäre, die Parameterwerte in der Abfrage fest zu codieren. Sie müssten dann die Abfrage jedes Mal ändern, wenn Sie einen anderen

Parameterwert verwenden wollten. Sie können auch mehrere Berichte mit einem unterschiedlichen in der Abfrage definierten Wert erstellen.

Der Value Provider gibt an, wie der Parameterwert festgelegt ist, wenn der Benutzer den Bericht ausführt. In vielen Fällen ist der Value Provider eine UI-Komponente, die einen Wert oder eine Einstellung vom Benutzer akzeptiert. Beispielsweise können Sie den Value Provider eines Parameters als Dropdown-Liste mit gültigen Werten definieren, aus denen der Benutzer wählen kann. Außerdem können Sie den Value Provider als Textfeld definieren, das eine Zeichenkette akzeptiert, die der Benutzer eingibt. In einigen Fällen erfordert ein Parameter keinen Value Provider. Der Parameterwert wird ohne erforderliche Benutzeraktion automatisch festgelegt.

Diese Aufgabe ist ein Schritt beim Erstellen und Ändern von Notification Server-Berichten.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

So fügen Sie einem benutzerdefinierten Bericht einen Parameter hinzu

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Klicken Sie im linken Bereich auf den Bericht, den Sie bearbeiten möchten.
3. Klicken Sie oben rechts auf der Seite *"Berichtname"* auf "Bearbeiten".
4. Auf der Registerkarte "Berichtsparameter" haben Sie folgende Möglichkeiten:

So fügen Sie einen Parameter hinzu	Klicken Sie auf "Hinzufügen" und dann auf den gewünschten Abfrageparameter. Die Dropdown-Liste enthält alle Parameter, die in der Berichtsabfrage definiert, jedoch noch nicht dem Bericht hinzugefügt wurden.
So fügen Sie einen Parameter eines erweiterten Typs hinzu	Klicken Sie auf "Hinzufügen > Erweiterte Typen" und dann auf den gewünschten Typ.
So erstellen Sie einen neuen Parameter	■ Klicken Sie auf "Hinzufügen > Neuer Parameter". ■ Geben Sie im Dialogfeld "Parameter bearbeiten" unter "Parameter" die gewünschten Parametereinstellungen an. ■ Wählen Sie unter "Value Provider" in der Dropdown-Liste "Name" den Typ des gewünschten Value Provider aus. ■ Geben Sie unter "Konfiguration" die gewünschten Value Provider-Einstellungen an. ■ Klicken Sie auf "OK".

So ändern Sie einen Parameter

- Klicken Sie auf den zu ändernden Parameter und dann auf das Symbol "Bearbeiten".
- Geben Sie im Dialogfeld "Parameter bearbeiten" unter "Parameter" die gewünschten Parametereinstellungen an.
- Wählen Sie unter "Value Provider" in der Dropdown-Liste "Name" den Typ des gewünschten Value Provider aus.
  Die verfügbaren Optionen hängen von dem unter "Parameter" ausgewählten Parametertyp ab.
- Geben Sie unter "Konfiguration" die gewünschten Value Provider-Einstellungen an.
  Wenn Sie einen anderen Parameter in der Liste anzeigen oder bearbeiten möchten, klicken Sie auf den Pfeil nach oben bzw. nach unten, um die Details des entsprechenden Parameters anzuzeigen.
- Klicken Sie auf "OK".

5 Klicken Sie auf "Änderungen speichern".

Erstellen oder Ändern einer Diagrammansicht für einen benutzerdefinierten Bericht

Wenn Sie Ihren eigenen benutzerdefinierten Notification Server-Bericht erstellen oder ändern, können Sie eine Berichtansicht definieren. Die Berichtansicht ist die Art und Weise, wie Berichtergebnisse angezeigt werden. Wenn Sie verschiedene Ansichten für einen Bericht festlegen, können Sie die Berichtsergebnisse für unterschiedliche Benutzer anpassen. Mit einer Diagrammansicht können Sie Berichtsergebnisse in grafischer Form (z. B. Balken-, Linien-, Kreis- und Flächendiagramm) anzeigen.

Hinweis: Die Funktionen, die in den Diagrammansichten verwendet werden, werden von Tools eines anderer Herstellers zur Verfügung gestellt. Eine vollständige Beschreibung der Diagrammkomponenten finden Sie in der Dokumentation, die von Dundas Data Visualization, Inc. (Dundas.com) bereitgestellt werden.

Diese Aufgabe ist ein Schritt beim Erstellen und Ändern von Notification Server-Berichten.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

So erstellen bzw. ändern Sie eine Diagrammansicht für einen benutzerdefinierten Bericht

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Klicken Sie im linken Teilfenster auf den Bericht, den Sie bearbeiten möchten.
3. Klicken Sie auf der Seite *"Berichtname"* auf "Bearbeiten".
4. Führen Sie auf der Registerkarte "Ansichten" einen der folgenden Schritte aus:
   - Klicken Sie zum Erstellen einer neuen Diagrammansicht auf "Hinzufügen".
   - Wählen sie zum Ändern einer vorhandenem Diagrammansicht in der Dropdown-Liste "Ansicht" die gewünschte Ansicht.
5. (Optional) Geben Sie im Feld "Name" den Namen der Diagrammansicht ein.
6. Wählen Sie in der Dropdown-Liste "Typ" die Option "Diagramm".
7. Wählen Sie in der Dropdown-Liste "Diagrammtyp" den gewünschten Diagrammtyp aus.
8. Wählen Sie in der Dropdown-Liste "Diagrammstil" den gewünschten Stil aus.

   Ein Diagrammstil ist ein vordefinierter Satz von Farben, die für die Darstellung des Diagramms verwendet werden können.
9. Geben Sie in den Feldern "Größe" die Höhe und Breite des Diagramms in Pixel an.
10. Wählen Sie in der Dropdown-Liste "Diagrammbeschriftung" die gewünschte Option aus:

Alle	Zeigt die tatsächlichen Datenwerte und die Prozentsätze an.
Werte	Zeigt die tatsächlichen Datenwerte wie die Anzahl der Elemente für jeden Typ an.
Prozentsatz	Zeigt die Daten als Prozentsätze an, wie den Prozentsatz der Elemente für jeden Typ.
Keine	Keine Beschriftung wird angezeigt.
Nur X-Achse	Zeigt nur die Datenwerte für die X-Achse an. Die Y-Achse wird nicht gekennzeichnet.

11 Richten Sie die Diagrammansicht ein, indem Sie auf den folgenden Registerkarten die gewünschten Einstellungen angeben:

Titel	Geben Sie hier den Diagrammtitel und dessen Position an.
Legende	Geben Sie hier die Legende und deren Position an.
3D	Damit können Sie den 3D-Zoom einrichten. Mit Hilfe des 3D-Zooms können Sie ausgewählte Bereiche des Diagramms auf die volle Fenstergröße vergrößern.
X-Achse	Wählen Sie hier die Ergebnisspalte aus, die als X-Achse im Diagramm verwendet werden soll. Geben Sie den Titel an und konfigurieren Sie die Darstellung der X-Achse.
Y-Achse	Wählen Sie hier die Ergebnisspalte aus, die als Y-Achse im Diagramm verwendet werden soll. Geben Sie den Titel an und konfigurieren Sie die Darstellung der Y-Achse.

Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Ansichten" für eine Diagrammansicht" auf Seite 565.

Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann F1 drücken.

12 Klicken Sie auf "Änderungen speichern".

Erstellen oder Ändern einer Rasteransicht für einen benutzerdefinierten Bericht

Wenn Sie einen benutzerdefinierten Notification Server-Bericht erstellen oder ändern, können Sie die gewünschten Rasteransichten erstellen und ändern. Für jede Rasteransicht können Sie die Ergebnisspalten auswählen, die enthalten sein sollen, und angeben, wie die Ergebnisse formatiert werden.

Diese Aufgabe ist ein Schritt beim Erstellen und Ändern von Notification Server-Berichten.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

So erstellen bzw. ändern Sie eine Rasteransicht für einen benutzerdefinierten Bericht

1 Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".

2 Klicken Sie im linken Bereich auf den Bericht, den Sie bearbeiten möchten.

3 Klicken Sie oben rechts auf der Seite *"Berichtname"* auf "Bearbeiten".

4 Führen Sie auf der Registerkarte "Ansichten" einen der folgenden Schritte aus:

So erstellen Sie eine neue Rasteransicht	Klicken Sie auf "Hinzufügen".
So ändern Sie eine vorhandene Rasteransicht	Wählen Sie in der Dropdown-Liste "Ansicht" die Ansicht aus, die Sie ändern möchten.

5 (Optional) Geben Sie im Feld "Name" den Namen der Ansicht ein.

6 Wählen Sie in der Dropdown-Liste "Typ" die Option "Raster" aus.

7 Geben Sie auf der Registerkarte "Ausgeblendete Spalten" die Datenspalten an, die in die Rasteransicht des benutzerdefinierten Berichts aufgenommen werden sollen.

Standardmäßig enthält die Rasteransicht alle Spalten in den Abfrageergebnissen. Sie können Datenspalten, die für den Benutzer nicht sichtbar sein sollen, ausblenden.

8 Richten Sie auf der Registerkarte "Erweiterte Formatierung" eine Formatierungsvorlage ein, mit der geeignete Zellen oder Zeilen in den Berichtergebnissen mit HTML formatiert werden.

Beispielsweise können Sie in einem Bericht über den Festplattenspeicher alle Computer hervorheben, deren verfügbarer Speicher unterhalb eines bestimmten Minimums liegt. Mit einer eigens erstellten Vorlage werden die relevanten Zeilen mit einem gelben Hintergrund versehen, und in den Zellen mit der Angabe zum freien Speicherplatz wird Fettschrift verwendet.

Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Ansichten" für eine Rasteransicht" auf Seite 568.

Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann F1 drücken.

9 (Optional) Klicken Sie zum Anzeigen einer Vorschau des Rasters mit den aktuellen Einstellungen auf "Vorschau".

10 Klicken Sie auf "Änderungen speichern".

Einrichten der Drilldown-Aktionen für einen benutzerdefinierten Bericht

Wenn Sie einen eigenen benutzerdefinierten Notification Server-Bericht erstellen oder ändern, können Sie einen Berichts-Drilldown einrichten. Ein Bericht-Drilldown ist eine Aktion, die durchgeführt wird, wenn der Benutzer auf ein Element in den Berichtergebnissen klickt. Es empfiehlt sich, Drilldowns für einen Bericht zu

konfigurieren, damit der Benutzer zusätzliche Informationen durch die Berichtergebnisse beziehen kann. Wenn Sie einen Drilldown für ein Element ausführen, wird die zugehörige Ansicht geöffnet. Bei dieser kann es sich um einen weiteren Bericht oder eine URL-Adresse handeln (wie beispielsweise die Ressourcenmanager-Konsole).

Um verschiedene Aktionen für verschiedene Ressourcentypen durchzuführen, können Sie in einem Bericht mehrere Drilldowns einrichten.

Für jeden Drilldown können Sie die Ansicht angeben, auf der der Drilldown verfügbar ist, und auch angeben, wie der Benutzer den Drilldown auslöst. Sie können auch die Aktion, die durchgeführt wird, und die für die Aktion verwendeten Parameter festlegen.

Sie können mehrere Drilldown-Berichte erstellen, d. h. Gruppen von Berichten, die in einer Hierarchiestruktur verknüpft sind. Anhand diese Struktur können Sie ein ein Element in einem Berichtsergebnissatz auswählen und weitere Berichte darauf ausführen. Drilldown-Berichte können erweiterte Informationen für kleinere Ressourcensätze darstellen oder unterschiedliche Informationen über die Ressource durch Berichterstellung zu verschiedenen Feldern zur Verfügung stellen.

Diese Aufgabe ist ein Schritt beim Erstellen und Ändern von Notification Server-Berichten.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

So richten Sie Drilldown-Aktionen für einen benutzerdefinierten Bericht ein

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Klicken Sie im linken Teilfenster auf den Bericht, den Sie bearbeiten möchten.
3. Klicken Sie auf der Seite *"Berichtname"* auf "Bearbeiten".
4. Führen Sie auf der Registerkarte "Drilldowns" einen der folgenden Schritte aus:

So fügen Sie einen neuen Drilldown hinzu	Klicken Sie auf "Hinzufügen".
So ändern Sie einen vorhandenen Drilldown	Wählen Sie in der Dropdown-Liste "Drilldown" den Drilldown aus, den Sie ändern möchten.

5. Geben Sie im Feld "Name" einen entsprechenden Namen für den Drilldown ein.

6 Geben Sie unter "Aktions-Wireup" die folgenden Einstellungen an:

Verfügbar auf	Geben Sie hier die gewünschte Berichtsansicht an.
Ereignis	Geben Sie hier das zum Ausführen des Drilldown erforderliche Benutzerereignis an.
Durchführen	Geben Sie hier die Aktion an, die der Drilldown durchführt. Abhängig von der ausgewählten Aktion ändern sich die Optionen unter "Aktionskonfiguration".

7 Geben Sie unter "Aktionskonfiguration" Folgendes an:

Drilldown bis Bericht	Wählen Sie in der Dropdown-Liste "Berichtelement" den Bericht aus, der von der Drilldown-Aktion ausgeführt werden soll.
Kontextmenü anzeigen	Nicht anwendbar
URL in neuem Fenster öffnen	Geben Sie im Feld "URL öffnen" die URL des Elements ein, das von der Drilldown-Aktion geöffnet werden soll, und klicken Sie dann auf "Einstellen".
URL in neuem Fenster für Remote-NS öffnen	Geben Sie im Feld "Remote-Berichtelement-GUID:" die GUID des Remote-Berichts ein, die von der Drilldown-Aktion geöffnet werden soll, und klicken Sie dann auf "Einstellen".

8 Richten Sie unter "Parameter werden übergeben" die Parameter ein, die Werte an die Drilldown-Aktion übergeben.

Aktivieren oder bearbeiten Sie die folgenden Optionen des Parameters:

Quelle	Die Quelle des Parameterwerts: ■ Benannter Parameter ■ Erster ausgewählter Wert ■ Ausgewählte Reihe ■ Gesamte Auswahl
Feldinfos	Der Name des Quellfelds.
Zielparameter	Der Name des Parameters.

Zielparametertyp	Der Parametertyp. Die Dropdown-Liste enthält alle verfügbaren Parametertypen.

Sie müssen Eigenschaften oder Werte des ausgewählten Elements an die Parameter in der Drilldown-Aktion anpassen. So wird gewährleistet, dass die geeigneten Schritte durchgeführt werden. Beispiel: Wenn mit Hilfe der Drilldown-Aktion der Ressourcenmanager geöffnet werden soll, können Sie die entsprechende Ressourcen-GUID als Parameter übergeben. Soll die Drilldown-Aktion einen Bericht ausführen, können Sie die entsprechenden Werte für die Berichtsabfrage übergeben.

9 Klicken Sie auf "Änderungen speichern".

Festlegen der erweiterten Eigenschaften eines benutzerdefinierten Berichts

Wenn Sie einen benutzerdefinierten Notification Server-Bericht erstellen oder ändern, können Sie die Berichtergebnisse auf den Benutzer einschränken, der den Bericht ausführt. Standardmäßig werden bei der Ausführung von Berichten alle Ergebnisse (bereichlos) aus der CMDB abgerufen. Die Berichtergebnisse können dann auf einen Bereich festgelegt werden, um sicherzustellen, dass der Benutzer nur für ihn geeignete Daten einsehen kann. Diese Bereichszuordnung kann aber auch auf den Bericht angewendet werden, damit nur entsprechende Daten aus der CMDB extrahiert werden.

Sie können auch wählen, den Bericht nur als Snapshot auszuführen. Um die Belastung des Notification Server zu minimieren, können Sie große oder häufig verwendete Berichte als Snapshots ausführen. Wenn ein Benutzer den Bericht ausführt, werden die Ergebnisse vom neuesten Snapshot abgerufen, anstatt dass die Berichtsabfrage auf dem CMDB ausgeführt wird. Wenn Sie einen Bericht nur als Snapshot einrichten, können optional Sie das Höchstalter des Snapshots angeben. Wenn der Snapshot dieses Alter erreicht, wird die Berichtsabfrage auf CMDB ausgeführt, um die neuesten Ergebnisse zu extrahieren und den Snapshot zu aktualisieren.

Diese Aufgabe ist ein Schritt beim Erstellen und Ändern von Notification Server-Berichten.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

So geben Sie erweiterte Eigenschaften eines benutzerdefinierten Berichts an

1. Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".
2. Klicken Sie im linken Teilfenster auf den Bericht, den Sie bearbeiten möchten.
3. Klicken Sie auf der Seite *"Berichtname"* auf "Bearbeiten".
4. Auf der Registerkarte "Erweitert" haben Sie folgende Möglichkeiten:

So stufen Sie Bereichsinformationen zur Datenquelle herauf	Aktivieren Sie "Bereichsinformationen zur Datenquelle heraufstufen".
So führen Sie den Bericht nur als Snapshot aus	1. Aktivieren Sie "Bericht immer als Snapshot ausführen". 2. Geben Sie im Feld "Snapshot automatisch aktualisieren, wenn älter als" das Alter an, an dem der Snapshot mit den neuesten Berichtergebnissen aktualisiert werden soll.

5. Klicken Sie auf "Änderungen speichern".

Kapitel 30

Anzeigen von Ressourceninformationen

In diesem Kapitel werden folgende Themen behandelt:

- Informationen zu Ressourcen
- Anzeigen von Ressourcendatenklasseinformationen
- Anzeigen von Ressourcenzuordnungstypinformationen
- Anzeigen von Ressourcentypinformationen

Informationen zu Ressourcen

Ressourcen sind diejenigen Elemente, mit denen Notification Server arbeitet und Daten über sie speichert, wie beispielsweise Assets, Rechnungen, Bestellungen, Projekte, Verträge und Benutzer. Daten über eine Ressource werden mithilfe einer Vorlage, dem sog. Ressourcentyp, der Configuration Management Database (CMDB) hinzugefügt. Jede Ressource in CMDB hat einen Ressourcentyp, der die Informationen angibt, die über die Ressource aufgezeichnet werden. Beispielsweise Ressourcenname, Beschreibung, Modell, Asset-Tag-Nummer, Besitzer, Abteilung usw.

Je größer die Zahl der Ressourcen ist, mit denen Sie arbeiten, desto mehr müssen Sie Ressourcen für Verwaltungszwecke zusammen gruppieren. Sie können Organisationsansichten, Organisationsgruppen und Ressourcenfilter verwenden, um zum Gruppieren Ihrer Ressourcen beizutragen.

Siehe "Anzeigen von Ressourcendatenklasseinformationen" auf Seite 492.

Siehe "Anzeigen von Ressourcenzuordnungstypinformationen" auf Seite 492.

Siehe "Anzeigen von Ressourcentypinformationen" auf Seite 492.

Anzeigen von Ressourcendatenklasseinformationen

Sie können Ressourcendatenklasseinformationen anzeigen. Eine Ressourcendatenklasse definiert eine oder mehrere Felder sowie die Eigenschaften der Felder, die eine Ressource dieser Klasse haben kann.

Siehe "Informationen zu Ressourcen" auf Seite 491.

So zeigen Sie Ressourcendatenklasseninformationen an

1. Klicken Sie in der "Symantec Management Console" im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster den Ordner "Einstellungen" >" Notification Server" > "Einstellungen für Ressourcen und Datenklassen" > "Datenklassen" und wählen Sie die entsprechende Datenklasse aus.

Anzeigen von Ressourcenzuordnungstypinformationen

Sie können Ressourcenzuordnungstypinformationen anzeigen. Eine Ressourcenzuordnung ist eine Verknüpfung zwischen zwei Ressourcen (z. B. zwischen einem Benutzer und einem Computer). Der Benutzer eines Computers ist diesem Computer zugeordnet und umgekehrt.

Siehe "Informationen zu Ressourcen" auf Seite 491.

So zeigen Sie Ressourcenzuordnungstypinformationen an

1. Klicken Sie in der "Symantec Management Console" im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster den Ordner "Einstellungen" >" Notification Server" > "Einstellungen für Ressourcen und Datenklassen" > "Ressourcenzuordnungen" und wählen Sie die gewünschte Ressourcenzuordnung aus.

Anzeigen von Ressourcentypinformationen

Sie können Ressourcentypinformationen (z. B. den Basisressourcentyp und die Ressourcenzuordnungen, die für den Ressourcentyp gelten) anzeigen. Außerdem können Sie die Datenklassen anzeigen, die im Ressourcentyp enthalten sind.

Siehe "Informationen zu Ressourcen" auf Seite 491.

So zeigen Sie Ressourcentypinformationen an

1. Klicken Sie in der "Symantec Management Console" im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster den Ordner "Einstellungen" >" Notification Server" > "Einstellungen für Ressourcen und Datenklassen" > "Ressourcentypen" und wählen Sie den gewünschten Ressourcentyp aus.
3. Zeigen Sie auf der Seite "Ressourcentyp - Informationen" auf der Registerkarte "Konfiguration" die folgenden Ressourcentypinformationen an:

Angaben zum Ressourcentyp	Ressourcentypname, Beschreibung und der Basisressourcentyp.
Zuordnungstypen	Ressourcenzuordnungen, die für den Ressourcentyp gelten. Standardmäßig werden nur die, die direkt angewendet wurden, angezeigt. Um alle Ressourcenzuordnungen anzuzeigen, aktivieren Sie "Geerbte Zuordnungstypen anzeigen".
Datenklassen	Die Datenklassen, die im Ressourcentyp enthalten sind. Standardmäßig werden alle Datenklassen angezeigt. So ändern Sie die Ansicht: 1 Klicken Sie auf eine der folgenden Optionen: Bearbeitbar: zeigt die bearbeitbaren Datenklassen an. Alle: zeigt alle Datenklassen an. Diese Auswahl wird auf die verfügbaren Datenklassen angewendet. 2 (Optional) Deaktivieren Sie zum Ausblenden geerbter Datenklassen die Option "Geerbte Datenklassen anzeigen".

Änderungen, die Sie vornehmen, werden nicht beibehalten, wenn Sie die Seite "Ressourcentyp - Informationen" verlassen. Die Standardeinstellungen werden wiederhergestellt, wenn Sie die Seite das nächste Mal öffnen.

Abschnitt 7

Verwalten von CMDB-Daten mit Data Connector

- Kapitel 31. Einführung in Data Connector
- Kapitel 32. Ausführen von Datenverwaltungsaufgaben

Kapitel 31

Einführung in Data Connector

In diesem Kapitel werden folgende Themen behandelt:

- Infos zu Data Connector
- Funktionsweise von Data Connector
- Einsatzmöglichkeiten von Data Connector

Infos zu Data Connector

Data Connector ist eine Komponente der Symantec Management-Plattform, mit der Sie Daten zwischen externen Datenquellen und der Configuration Management Database (CMDB) übertragen können. Sie können so Daten, die bereits in der CMDB oder anderen Anwendungen vorhanden sind, nutzen. Sie können Datenübertragungen planen, um Updates regelmäßig und automatisch auszuführen. Data Connector unterstützt viele Datenformate: OLEDB, ODBC, LDAP, XML und CSV.

Mit Data Connector können Sie auch die bereits in der CMDB enthaltenen Daten manipulieren. Daher können Sie Fehler in Ihren Daten normalisieren und korrigieren. Beispielsweise können Sie mit Data Connector Firmennamen angleichen.

Siehe "Funktionsweise von Data Connector" auf Seite 495.

Funktionsweise von Data Connector

Data Connector überträgt Daten mithilfe von Datenquelledefinitionen und Datenübertragungsregeln. Eine Datenquellendefinition definiert die Parameter für das Arbeiten mit einer bestimmten Datenquelle bzw. einem Datenempfänger. Zu

den Parametern gehören z. B. der Speicherort der Datenquelle, die Art der Datenübertragung und die zum Zugriff auf die Datenquelle erforderlichen Identifikationsdaten.

Data Connector unterstützt CSV-, LDAP-, ODBC-, OLEDB- und XML-Datenquellen.

Eine Datenübertragungsregel konfiguriert u. a. folgende Angaben:

- eine Datenquellendefinition, die für die Übertragung verwendet wird
- der bei der Übertragung genutzte Ressourcentyp
- Zuordnungen zwischen den bei der Übertragung genutzten Feldern
- ob die Übertragung ein Import oder ein Export ist

Für die einzelnen Arten der Datenübertragung sind entsprechende Regeln verfügbar:

Massenressourcenexport	Eine effiziente Möglichkeit zum Exportieren von Massenressourcen aus einem Bericht oder einem Ressourcenziel in eine Notification Server-Ereignis-XML-Datei (NSE). Mit diesem Regeltyp können Sie auch Ressourcenänderungsverläufe exportieren.
Filterimportregel	Gibt die Mitgliedschaft im Symantec Management-Plattform-Filter durch Importieren der Filtermitgliedschaft aus einer Datenquelle an.
Regel für den Import der Organisationsgruppe	Gibt die Mitgliedschaft in Organisationsansichten und Gruppen der Symantec Management-Plattform durch Importieren der Organisationsansichts- oder Gruppenmitgliedschaft aus einer Datenquelle an.
Berichteexportregel	Exportiert Berichtsdaten in eine Datenquelle mit einer Datenquelledefinition, die das Exportieren zulässt.
Ressourcendatenübertragungsregel	Überträgt (importiert bzw. exportiert) die Ressourcendaten zwischen einer Datenquelle und der CMDB.

Zum Automatisieren der Datenübertragung können Sie angeben, dass die Datenübertragungsregeln zu einem bestimmten Zeitpunkt ausgeführt werden sollen. Datenübertragungsregeln können auch über Symantec Management-Plattform-Aufgaben ausgeführt werden. Nach den Datenübertragungen können Sie vordefinierte Berichte und Protokolldateien verwenden, um die Ergebnisse der Datenübertragung zu analysieren.

Mit Data Connector können Sie auch die bereits in der CMDB enthaltenen Daten mithilfe von CMDB-Regeln manipulieren. Mit diesen Regeln können Sie Daten normalisieren oder andere Konsistenzprobleme mit den CMDB-Daten beheben. Zum Bearbeiten der CMDB benötigen Sie CMDB Solution.

Siehe "Infos zu Data Connector" auf Seite 495.

Siehe "Einsatzmöglichkeiten von Data Connector" auf Seite 497.

Einsatzmöglichkeiten von Data Connector

Mit Data Connector können Sie Daten zwischen der CMDB und einer Datenquelle übertragen und in der CMDB bearbeiten.

Sie können folgende Datenübertragungsaktivitäten mit Data Connector durchführen:

- Übertragen (Import und Export) von Ressourcendaten zwischen einer Datenquelle und der CMDB
  Siehe "Importieren und Exportieren von Daten" auf Seite 498.
- Importieren von Filtermitgliedschaftsinformationen, einschließlich Hinzufügen bzw. Entfernen der Mitgliedschaft von Ressourcen aus einem oder mehreren Filtern
- Importieren von Organisationsansichts- und Gruppemitgliedschaften
- Exportieren von Berichten
- Massenexport von Ressourcen

Mit Data Connector können Sie auch Daten in der CMDB bearbeiten. Beispielsweise können Sie einen Datensatz in der CMDB normalisieren oder ändern. Zum Bearbeiten von Daten in der CMDB benötigen Sie CMDB Solution.

Kapitel 32

Ausführen von Datenverwaltungsaufgaben

In diesem Kapitel werden folgende Themen behandelt:

- Importieren und Exportieren von Daten
- Erstellen einer virtuellen Datenklasse
- Konfigurieren von Bereinigungsoptionen für die ausführliche Protokollierung in Data Connector

Importieren und Exportieren von Daten

Sie müssen einige Schritte durchführen, um die Daten zwischen der Configuration Management Database (CMDB) und einer Datenquelle zu übertragen.

Tabelle 32-1 So importieren und exportieren Sie Daten

Schritt	Aktion	Beschreibung
Schritt 1	Erstellen Sie eine Datendatei.	Zuerst müssen Sie eine Datendatei erstellen und diese mit Werten auffüllen. Sie können die Daten manuell oder über einen externen Vorgang eingeben. Wenn Sie Spaltenamen als erste Zeile in die Datendatei aufnehmen, können Sie mithilfe der Datenimportregel die Spalten den CMDB-Datenklassen zuweisen. Sie können auch die Daten in der externen Datenquelle vorbereiten, bevor Sie sie in die CMDB importieren. Siehe "Infos zum Vorbereiten von Daten vor dem Importieren" auf Seite 500.

Schritt	Aktion	Beschreibung
Schritt 2	Erstellen Sie eine Datenquelle.	Sie definieren Datenquellen unter Verwendung von Datenquellendefinitionen. Datenquellendefinitionen definieren die Parameter, die angegeben werden müssen, damit mit der Datenquelle gearbeitet werden kann. Beispielsweise kann eine Datenquellendefinition Speicherorte von Datenbanken oder Dateien, Servernamen und Identifikationsdaten definieren. Siehe "Erstellen einer Datenquellendefinition" auf Seite 500.
Schritt 3	Erstellen Sie eine Datenübertragungsregel.	Mit der Datenübertragungsregel können Sie die Datenübertragung konfigurieren. Datenübertragungsregeln geben die Parameter für die Datenübertragung an, zum Beispiel den Zeitplan für die Datenübertragung, die Eingabe- und Ausgabedatentabellenzuordnungen und die Richtung der Datenübertragung. Siehe "Erstellen einer Datenübertragungsregel" auf Seite 501.
Schritt 4	(Optional) Erstellen Sie einen Ressourcen-Suchschlüssel.	Ein Ressourcen-Suchschlüssel ist ein Satz von Datenklassenspalten zum Zuordnen der Ressourcen in der CMDB und der Datenquelle. Siehe "Erstellen eines Ressourcen-Suchschlüssels" auf Seite 502.
Schritt 5	(Optional) Führen Sie die Datenübertragungsregel als Aufgabe aus.	Sie können eine Aufgabe zum Ausführen der Datenübertragungsregel planen. Siehe "Ausführen einer Datenübertragungsregel als Aufgabe" auf Seite 503.
Schritt 6	Prüfen Sie die Ergebnisse der Datenübertragung.	Sie können vordefinierte Berichte verwenden, um zu überprüfen, ob die Datenübertragung erfolgreich war. Siehe "Anzeigen von Datenübertragungsübersichten" auf Seite 504.
Schritt 7	(Optional) Prüfen Sie die Funktionsweise der Datenübertragungsregel.	Sie können die Funktionsweise von Datenübertragungsregeln prüfen. Dabei wird gewährleistet, dass es keine Probleme gibt, die durch Änderungen an der Regel verursacht werden und verhindern, dass die Datenübertragung erfolgreich durchgeführt wird. Siehe "Prüfen der Funktionsweise von Datenübertragungsregeln" auf Seite 504.

Schritt	Aktion	Beschreibung
Schritt 8	(Optional) Verwalten Sie die importierten Daten.	Sie können CMDB-Regeln zum Bereinigen, Normalisieren oder Erstellen von Massenänderungen an den Daten in der CMDB erstellen. Siehe "Erstellen einer CMDB-Regel zum Bearbeiten von CMDB-Daten" auf Seite 505. Siehe "Ausführen einer CMDB-Regel als Aufgabe" auf Seite 506.

Infos zum Vorbereiten von Daten vor dem Importieren

Wenn Sie Daten aus einer externen Datenquelle in die Configuration Management Database (CMDB) importieren, können Sie die Daten manipulieren, bevor die Daten importiert werden. Auf diese Weise können Sie die Daten bearbeiten, ohne sie in der Datenquelle selbst zu ändern.

Sie schreiben eine Datenvorbereitungsfunktion in C#. Wie viel Sie vorbereiten können hängt vom Funktionsumfang der Programmiersprache C# ab. Eine Datenvorbereitungsfunktion in C# nimmt eine Datentabelle als Eingabeparameter. Sie können C#-Code schreiben, um die Datentabelle und ihren Inhalt zu manipulieren. Eine aktualisierte Datentabelle wird dann als der Rückgabewert der Methode ausgegeben. Die ausgegebene Datentabelle sind die Daten, die aus der Datenquelle importiert werden.

Ein Beispiel zum besseren Verständnis: Eine OLEDB-Datenquelle ist so konfiguriert, dass "Tabelle A" aus "Datenbank A" verwendet wird. Eine Vorbereitungsfunktion fügt dynamisch eine neue Spalte in die Tabelle ein. Sie füllt außerdem die neue Spalte mit den Daten, die aus anderen Spalten der Tabelle abgeleitet wurden.

Diese Aufgabe ist ein optionaler Schritt beim Importieren und Exportieren von Daten.

Siehe "Importieren und Exportieren von Daten" auf Seite 498.

Erstellen einer Datenquellendefinition

Eine Datenquelle ist eine Quelle oder ein Empfänger von Configuration Management Database(CMDB)-Daten. Beispielsweise können eine CSV-Datei oder eine ODBC-Datenbank eine Datenquelle sein.

Sie können Daten zwischen den folgenden Datenquellentypen und der CMDB übertragen:

- CSV
- LDAP
- ODBC

- OLEDB
- XML
- Benutzerdefiniert

Eine Datenquellendefinition gibt an, wie auf eine bestimmte Datenquelle zugegriffen wird. Die Definition enthält den Datenquellentyp, den Speicherort, den Tabellennamen und Authentifizierungsinformationen. Sie benötigen für jede Datenquelle, an die bzw. aus der Sie Daten übertragen möchten, eine Datenquellendefinition. Für verschiedene Datenquellentypen gibt es verschiedene Datenquellendefinitionstypen. Manche Datenquellendefinitionstypen ermöglichen das Importieren und Exportieren von Daten aus der CMDB. Andere Typen ermöglichen nur das Exportieren oder Importieren.

Sie müssen eine Datenquellendefinition für alle Datenquellen erstellen, zwischen denen Daten übertragen werden sollen.

Diese Aufgabe ist ein Schritt beim Importieren und Exportieren von Daten.

Siehe "Importieren und Exportieren von Daten" auf Seite 498.

So erstellen Sie eine Datenquellendefinition

1. Klicken Sie in Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster "Einstellungen > Notification Server > Connector".
3. Klicken Sie mit der rechten Maustaste auf "Datenquellen" und dann auf "Neu > *Datenquelle"*.
4. Geben Sie im rechten Teilfenster die entsprechenden Werte an.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.
5. (Optional) Klicken Sie auf "Datenquelle testen", um den Zugriff auf die Datenquelle zu prüfen.
6. Klicken Sie auf "Änderungen speichern".

Erstellen einer Datenübertragungsregel

Bevor Sie Daten zwischen der Configuration Management Database (CMDB) und einer Datenquelle übertragen können, müssen Sie die Optionen für die Datenübertragung angeben. Beispielsweise müssen Sie Folgendes angeben:

- Welche Art von Daten übertragen wird
- Ob die Daten importiert oder in die Datenquelle exportiert werden

- Welche Daten aus der Datenquelle übertragen werden
- Wann die Datenübertragung stattfindet

Zum Angeben der Optionen für eine Datenübertragung verwenden Sie eine Datenübertragungsregel. Es ist eine Reihe verschiedener Datenübertragungsregeln verfügbar. Welche Sie verwenden, hängt vom Typ der zu übertragenden Daten ab.

Bevor Sie eine Datenübertragungsregel in einer Produktionsumgebung einsetzen, sollten Sie sie testen. Verwenden Sie dazu die Option "Regel testen" auf der Seite der entsprechenden Datenübertragungsregel.

Diese Aufgabe ist ein Schritt beim Importieren und Exportieren von Daten.

Siehe "Importieren und Exportieren von Daten" auf Seite 498.

So erstellen Sie eine Datenübertragungsregel

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster "Einstellungen > Notification Server > Connector".
3. Klicken Sie mit der rechten Maustaste auf "Import-/Exportregeln" und klicken Sie auf "Neu > *Datenübertragungsregel"*.
4. Geben Sie im rechten Teilfenster die Spaltenzuordnungen und einen Zeitplan für die Regel an.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.
5. Klicken Sie auf "Änderungen speichern".

Erstellen eines Ressourcen-Suchschlüssels

Ein Ressourcen-Suchschlüssel ist ein eindeutiger Wert für einen Ressourcentyp, der zum Abgleichen der Ressourcen in der CMDB (Configuration Management Database) und der Datenquelle verwendet wird.

Diese Aufgabe ist ein Schritt beim Importieren und Exportieren von Daten.

Siehe "Importieren und Exportieren von Daten" auf Seite 498.

So erstellen Sie einen Ressourcensuchschlüssel

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster "Einstellungen > Notification Server > Connector".

3 Klicken Sie mit der rechten Maustaste auf "Ressourcen-Suchschlüssel" und klicken Sie dann auf "Neu > Ressourcen-Suchschlüssel".

4 Geben Sie im rechten Teilfenster die folgenden Einstellungen an:

Zielressourcentyp	Ressourcentyp, für den der Suchschlüssel angegeben wird.
Datenklasse auswählen	Wählen Sie hier die Datenklasse aus, die den Wert enthält, den Sie als Suchschlüssel verwenden möchten.
In Schlüssel verwenden	Aktivieren Sie zum Angeben des Suchschlüssels die entsprechenden Kontrollkästchen.

5 Klicken Sie auf "Änderungen speichern".

Ausführen einer Datenübertragungsregel als Aufgabe

Sie können eine Datenübertragungsregel als Aufgabe ausführen. Wenn Sie eine Regel als Aufgabe ausführen, können Sie gleichzeitig weitere Aufgaben ausführen, die in einem einzelnen Auftrag enthalten sind.

Diese Aufgabe ist ein Schritt beim Importieren und Exportieren von Daten.

Siehe "Importieren und Exportieren von Daten" auf Seite 498.

So führen Sie eine Datenübertragungsregel als Aufgabe aus

1 Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Aufträge und Aufgaben".

2 Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, in dem die Aufgabe hinzugefügt werden soll, und klicken Sie auf "Neu > Auftrag oder Aufgabe".

3 Klicken Sie im linken Teilfenster des Dialogfelds "Neue Aufgabe erstellen" auf "Serveraufgaben > Connector-Regel ausführen".

4 Geben Sie im rechten Teilfenster einen Namen für die Aufgabe an und wählen Sie eine Datenübertragungsregel zum Ausführen der Aufgabe aus.

5 Klicken Sie auf "OK".

6 Geben Sie im rechten Teilfenster einen Zeitplan für das Ausführen der Regel an.

Siehe "Konfigurieren eines Zeitplans" auf Seite 129.

Siehe "Ausführen eines Jobs oder einer Aufgabe" auf Seite 442.

Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.

Anzeigen von Datenübertragungsübersichten

Sie können die Ergebnisse von Datenübertragungen (z. B. Ressourcenzählungen, Zeilenzählungen, Übertragungszeiten und -Daten sowie Datenquellen) durch vordefinierte Berichte anzeigen. Diese Berichte können beim Verfolgen von Datenübertragungen nützlich sein.

Diese Aufgabe ist ein Schritt beim Importieren und Exportieren von Daten.

Siehe "Importieren und Exportieren von Daten" auf Seite 498.

So zeigen Sie Datenübertragungsübersichten an

1 Klicken Sie in der Symantec Management Console im Menü "Berichte" auf "Alle Berichte".

2 Im linken Teilfenster erweitern Sie "Berichte > Notification Server Management > Connector" und klicken auf den Bericht, den Sie anzeigen möchten.

Prüfen der Funktionsweise von Datenübertragungsregeln

Sie können die Funktionsweise aller Datenübertragungsregeln durch vordefinierte Aufgaben prüfen. Diese Zustandsprüfungsaufgaben testen alle Regeln. Dies entspricht dem Klicken auf "Regel testen" für die einzelnen Regelseiten.

Diese Zustandsprüfung hilft dabei, zu gewährleisten, dass die Regeln und die Datenquellendefinitionen richtig konfiguriert sind. Während der Prüfungen erkannte Fehler werden gemeldet und können im Aufgabenstatus der ausgeführten Zustandsprüfungsaufgaben angezeigt werden.

Die vordefinierten Aufgaben können wie andere Aufgaben so geplant werden, dass sie sofort, zu einem spezifischen Zeitpunkt oder regelmäßig ausgeführt werden.

Diese Aufgabe ist ein Schritt beim Importieren und Exportieren von Daten.

Siehe "Importieren und Exportieren von Daten" auf Seite 498.

So prüfen Sie die Funktionsweise von Datenübertragungsregeln

1. Klicken Sie in Symantec Management Console im Menü "Verwalten" auf "Jobs und Aufgaben".
2. Erweitern Sie im linken Teilfenster "Systemaufträge und -aufgaben > Notification Server > Connector" und klicken Sie dann auf "Aufgabe 'Zustandsprüfung der Connector-Regeln'" oder "Aufgaben 'Zustandsprüfung der CMDB-Regeln'".
3. Geben Sie im rechten Teilfenster einen Zeitplan für das Ausführen der Aufgabe an.

   Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.

   Siehe "Konfigurieren eines Zeitplans" auf Seite 129.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.
4. Nach dem Ausführen der Aufgabe können Sie im Abschnitt "Aufgabenstatus" den Zustand der einzelnen Datenübertragungsregeln anzeigen.

Erstellen einer CMDB-Regel zum Bearbeiten von CMDB-Daten

CMDB-Regeln sind benutzerdefinierten Regeln, die Sie zum Verwalten von Daten und Aufgaben erstellen können. Mit CMDB-Regeln können Sie die Daten manipulieren, die bereits in CMDB vorhanden sind. Mit diesen Regeln können Sie Daten normalisieren oder andere Konsistenzprobleme mit den CMDB-Daten beheben.

Sie können Ihre eigenen CMDB-Regeln erstellen, indem Sie eine Gruppe von Ressourcen basierend auf Typ und Eigenschaften als Ziel wählen und dann Änderungen vornehmen. Zum Erstellen einer Regel müssen Sie die Kriterien für die gewünschten Ressourcen, die vorzunehmenden Änderungen und die auszuführende Aktion definieren. Sie können die benutzerdefinierten CMDB-Regeln testen, bevor Sie sie in einer Produktionsumgebung ausführen, Zeitpläne erstellen und relevantes Personal benachrichtigen. CMDB-Regeln können auch unter Verwendung von Aufgaben und Aufträgen ausgeführt werden.

Beachten Sie, dass zum Einsatz von CMDB-Regeln die Anwendung "CMDB Solution" erforderlich ist.

Warnung: CMDB-Regeln sind leistungsstark und können große Datenmengen ändern. Bevor Sie eine CMDB-Regel in einer Produktionsumgebung einsetzen, empfiehlt Symantec dringend, unter Verwendung der Option "Regel testen" auf der Seite "CMDB-Regel" die Regel zunächst zu testen.

Diese Aufgabe ist ein Schritt beim Importieren und Exportieren von Daten.

Siehe "Importieren und Exportieren von Daten" auf Seite 498.

So erstellen Sie eine CMDB-Regel zum Bearbeiten von CMDB-Daten

1. Wählen Sie in der Symantec Management Console im Menü "Einstellungen" die Option "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster "Einstellungen > Notification Server > Connector".
3. Klicken Sie mit der rechten Maustaste auf CMDB-Regeln und klicken Sie auf Neu > CMDB-Regel.
4. Geben Sie im rechten Teilfenster Werte für die Regel an.

   Weitere Informationen erhalten Sie, indem Sie auf die Seite klicken und dann **F1** drücken.
5. Klicken Sie auf "Änderungen speichern".

Ausführen einer CMDB-Regel als Aufgabe

Sie können eine CMDB-Regel unter Verwendung einer Aufgabe ausführen, mit der Sie die Regel zusammen mit einer Reihe anderer Aufgaben in einem Job ausführen können.

Siehe "Erstellen einer CMDB-Regel zum Bearbeiten von CMDB-Daten" auf Seite 505.

Hinweis: Benutzerdefinierte Aufgaben aus Connector Solution 6.5 werden nicht automatisch in das aktuelle Produkt migriert. Sie müssen diese Aufgaben manuell neu erstellen. Außerdem wurde die Funktion zum Ausführen mehrerer Regeln durch eine Aufgabe in einer angegebenen Reihenfolge in die Jobs verschoben. Jede Aufgabe kann jeweils nur eine Regel ausführen.

Diese Aufgabe ist ein Schritt beim Importieren und Exportieren von Daten.

Siehe "Importieren und Exportieren von Daten" auf Seite 498.

So führen Sie eine CMDB-Regel als Aufgabe aus

1. Wählen Sie in der Symantec Management Console im Menü "Verwalten" die Option "Aufträge und Aufgaben".
2. Klicken Sie im linken Teilfenster mit der rechten Maustaste auf den Ordner, in dem die Aufgabe hinzugefügt werden soll, und klicken Sie auf "Neu > Auftrag oder Aufgabe".
3. Klicken Sie im linken Teilfenster des Dialogfelds "Neue Aufgabe erstellen" auf "Serveraufgaben > CMDB-Regel ausführen".

4 Geben Sie im rechten Teilfenster einen Namen für die Aufgabe an und wählen Sie eine CMDB-Regel zum Ausführen der Aufgabe aus.

5 Klicken Sie auf "OK".

6 Geben Sie im rechten Teilfenster einen Zeitplan für das Ausführen der Regel an.

Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.

Siehe "Konfigurieren eines Zeitplans" auf Seite 129.

Erstellen einer virtuellen Datenklasse

Mit virtuellen Datenklassen können Sie Systemsdaten anderer Hersteller in die Symantec Management-Plattform-CMDB aufnehmen, ohne die Daten in die CMDB importieren zu müssen.

Externe Daten, die einer virtuellen Datenklasse zugeordnet sind, werden wie eine normale Ressourcendatenklasse in der CMDB angezeigt. Virtuelle Datenklassen ermöglichen eine nahtlose Integration mit den Berichterstellungsfunktionen der Symantec Management-Plattform. Sie können den Berichtgenerator verwenden, um die Ressourcenberichte basierend auf virtuellen Datenklassen zu erstellen. Der Bericht fragt die Daten direkt aus der externen Datenquelle ab, wenn Sie den Bericht ausführen.

Diese Verbindungsserver müssen zuerst in SQL Server eingerichtet werden, bevor Sie virtuelle Datenklassen verwenden können. Weitere Informationen finden Sie in der Microsoft-Dokumentation zu Verbindungsservern unter http://msdn.microsoft.com/en-us/library/ms188279(SQL.90).aspx.

Sie benötigen das Recht "Data Connector verwalten", um virtuelle Datenklassen erstellen, bearbeiten oder löschen zu können. Zum Bearbeiten einer virtuellen Datenklasse benötigen Sie außerdem Schreibzugriff.

So erstellen Sie eine bearbeitbare virtuelle Datenklasse

1 Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".

2 Erweitern Sie im linken Teilfenster "Einstellungen > Notification Server > Einstellungen für Ressourcen und Datenklassen".

3 Klicken Sie mit der rechten Maustaste auf "Datenklassen" und klicken Sie dann auf "Neu > Virtuelle Datenklasse".

4 Klicken Sie auf "Änderungen speichern".

Konfigurieren von Bereinigungsoptionen für die ausführliche Protokollierung in Data Connector

Sie können das Bereinigen von Regelprotokolldateien konfigurieren. Das Bereinigen wird während des täglichen Standardzeitplans durchgeführt.

So konfigurieren Sie Bereinigungsoptionen für die ausführliche Protokollierung in Data Connector

1. Klicken Sie in der Symantec Management Console im Menü "Einstellungen" auf "Alle Einstellungen".
2. Erweitern Sie im linken Teilfenster "Einstellungen > Notification Server > Connector" und klicken Sie anschließend auf "Connector-Bereinigungsrichtlinie".
3. Geben Sie im rechten Teilfenster die Bereinigungsoptionen an.
4. Klicken Sie auf "Änderungen speichern".

Anhang A

Sicherheitsrechte und -berechtigungen

Dieser Anhang enthält folgende Themen:

- Sicherheitsprivilegkategorien
- Kategorien von Sicherheitsberechtigungen
- Verbindungsprofil-Privilegien
- Verwaltungsrechte
- Systemrechte
- Identifikationsdatenprivilegien
- Workflow-Verzeichnisprivilegien
- Symantec Management Console-Rechte
- Software Management-Rechte
- Kontextmenü-Privilegien
- Kontextmenü: Privilegien für Connector-Beispiele
- Kontextmenü: Hierarchie-Privilegien
- Kontextmenü - Privilegien "Aktionen"
- Kontextmenü: Privilegien zum Einstellen des Asset-Status
- Ressourcenverwaltungsberechtigungen
- Systemberechtigungen

- Task Server-Berechtigungen
- Berichtsberechtigungen
- Richtlinienberechtigungen
- Ordnerberechtigungen
- Filterberechtigungen
- Verbindungsprofil-Berechtigungen
- Credential Manager-Berechtigungen

Sicherheitsprivilegkategorien

Ein Recht ermöglicht einem Benutzer die Ausführung einer bestimmten Aktion auf der Symantec Management-Plattform oder an Elementen in der Symantec Management Console. Damit der Benutzer eine Aktion an einem Element ausführen kann, muss seine Rolle die notwendige Berechtigung für das Element haben. Die Privilegien, die Sie Sicherheitsrollen zuweisen können, sind in Kategorien unterteilt. Wenn Sie jedoch einer Sicherheitsrolle Privilegien zuweisen, müssen Sie die entsprechenden Privilegien einzeln auswählen.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-1 Sicherheitsprivilegkategorien

Privilegkategorie	Beschreibung
Verbindungsprofil-Privilegien	Zum Erstellen und Ändern von Verbindungsprofilen. Siehe "Verbindungsprofil-Privilegien" auf Seite 513.
Managementprivilegien	Zum Erstellen von Verwaltungselementen wie Filtern, Zielen, Berichten und Aufgaben in der Symantec Management-Plattform. Siehe "Verwaltungsrechte" auf Seite 514.
Systemprivilegien	Zum Ausführen von Verwaltungsaktivitäten wie Einrichten der Sicherheit, Verwalten der Hierarchie und Importieren von XML-Dateien in der Symantec Management-Plattform. Siehe "Systemrechte" auf Seite 516.

Privilegkategorie	Beschreibung
Identifikationsdatenprivilegien	Zum Verwenden des Credential Manager, um Identifikationsdaten zu erstellen und zu ändern. Diese Identifikationsdaten sind nicht dasselbe wie die internen Identifikationsdaten und die Windows-Identifikationsdaten, die mit Benutzerkonten verknüpft sind. **Hinweis:** Der Credential Manager ist eine Komponente der erweiterten Symantec Management-Plattform, also in Ihrer Umgebung möglicherweise nicht installiert. Siehe "Identifikationsdatenprivilegien" auf Seite 518.
Workflow-Privilegien	Zum Veröffentlichen von Workflows aus Workflow Designer in Notification Server als Aufgabe oder Elementaktion (eine Option im Kontextmenü). Siehe "Workflow-Verzeichnisprivilegien" auf Seite 519.
Konsolenprivilegien	Zum Anpassen der Symantec Management Console. Diese Privilegien umfassen die Bearbeitung von Menüs sowie die Erstellung von Portalseiten, Web-Parts und Ansichten. Siehe "Symantec Management Console-Rechte" auf Seite 519.
Software Management-Rechte	Hier können Sie bestimmte Fähigkeiten der Benutzerrolle zuweisen und der Benutzer kann bestimmte Aufgaben in der Ansicht "Software" und im Fenster "Softwarekatalog" durchführen. Mit diesen Privilegien können Sie die Softwarebibliothek erstellen sowie Softwareressourcen erstellen und importieren. Siehe "Software Management-Rechte" auf Seite 521.
Kontextmenü-Privilegien	Zum Ausführen allgemeiner Aktionen an Elementen in der Symantec Management Console. Wenn Sie mit der rechten Maustaste auf ein Element klicken, sind die für diesen Elementtyp relevanten Optionen im Kontextmenü verfügbar. Diese Privilegien erlauben das Löschen von Elementen, die Bearbeitung von Ansichten, Weblinks und Elementlinks sowie das Starten, Anhalten und Planen von Aufgaben. Siehe "Kontextmenü-Privilegien" auf Seite 522.
Kontextmenü: Privilegien für Connector-Beispiele	Beispiele für von Benutzern erstellbare Kontextmenüaktionen. Siehe "Kontextmenü: Privilegien für Connector-Beispiele" auf Seite 524.
Kontextmenü: Hierarchie-Privilegien	Zum Verwalten der Hierarchiereplikation. Diese Privilegien ermöglichen den Ein- bzw. Ausschluss bestimmter Elemente bei der Hierarchiereplikation sowie die sofortige Replikation von Elementen. Siehe "Kontextmenü: Hierarchie-Privilegien" auf Seite 524.
Kontextmenü - Privilegien "Aktionen"	Zum Ausführen von für das Software Management Framework relevanten Aktionen. Für zusätzliche Lösungen, die auf der Symantec Management-Plattform installiert werden, können ggf. weitere Privilegien dieser Kategorie hinzugefügt werden. Siehe "Kontextmenü: Hierarchie-Privilegien" auf Seite 524.

Privilegkategorie	Beschreibung
Kontextmenü: Privilegien zum Einstellen des Asset-Status	Zum Ändern des Status von Assets. Mit diesen Privilegien können Sie den Status einer Ressource auf "Aktiv" oder "Stillgelegt" setzen. Lösungen, die auf der Symantec Management-Plattform installiert werden, fügen möglicherweise weitere Privilegien hinzu. Siehe "Kontextmenü: Privilegien zum Einstellen des Asset-Status" auf Seite 527.

Kategorien von Sicherheitsberechtigungen

Die Berechtigungen für ein Element in Symantec Management Console legen den Zugriff fest, den eine Sicherheitsrolle auf dieses Element hat. Berechtigungen für Elemente werden auf Sicherheitsrollen und nicht auf einzelne Benutzerkonten angewendet. Beispielsweise kann ein Benutzer mit der Leseberechtigung für ein Element das Element anzeigen und es mit der Schreibberechtigung für das Element ändern.

Siehe "Zuweisen von Sicherheitsberechtigungen zu Ordnern und Elementen" auf Seite 108.

Berechtigungen werden mit Privilegien verwendet, um festzulegen, welche Aktionen eine Sicherheitsrolle an einem Element durchführen kann. Beispielsweise muss eine Sicherheitsrolle zum Löschen eines Elements das Recht zum Löschen sowie die Berechtigung zum Löschen dieses bestimmten Elements haben. Es genügt nicht, nur das Recht zum Löschen oder die Berechtigung zum Löschen dieses Elements zu haben.

Sie können die Berechtigungen angeben, die für jeden Ordner oder jedes Element für jede Sicherheitsrolle gelten. Berechtigungen, die direkt auf einen Ordner oder ein Element angewendet werden (nicht geerbte Berechtigungen), werden mit den Berechtigungen kombiniert, die vom übergeordneten Ordner geerbt werden. Die kombinierten Berechtigungen legen den Zugriff fest, den die Sicherheitsrolle für den betreffenden Ordner bzw. das Element hat.

Standardmäßig erben untergeordnete Elemente und Ordner alle Berechtigungen für einen Ordner. Sie können die Berechtigungsvererbung Ihren Anforderungen entsprechend ändern.

Es ist eine Reihe von Kategorien für Sicherheitsberechtigungen für jede Rolle verfügbar.

Tabelle A-2 Kategorien von Sicherheitsberechtigungen

Berechtigungskategorie	Beschreibung
Ressourcenverwaltung	Diese Berechtigungen gelten für Ressourcen. Siehe "Ressourcenverwaltungsberechtigungen" auf Seite 527.
System	Diese Berechtigungen gelten für das System, z. B. das Lesen, Schreiben und Löschen von Elementen. Siehe "Systemberechtigungen" auf Seite 528.
Task Server	Diese Berechtigungen gelten für Task Server. Siehe "Task Server-Berechtigungen" auf Seite 528.
Bericht	Diese Berechtigungen gelten für Berichte. Siehe "Berichtsberechtigungen" auf Seite 529.
Richtlinie	Diese Berechtigungen gelten für Richtlinien. Siehe "Richtlinienberechtigungen" auf Seite 529.
Ordner	Diese Berechtigungen gelten für Ordner. Siehe "Ordnerberechtigungen" auf Seite 529.
Filter	Diese Berechtigungen gelten für Filter. Siehe "Filterberechtigungen" auf Seite 530.
Verbindungsprofil	Diese Berechtigungen ermöglichen die Verwendung von Verbindungsprofilen. Siehe "Verbindungsprofil-Berechtigungen" auf Seite 530.
Credential Manager	Diese Berechtigungen ermöglichen die Verwendung des Credential Manager. Siehe "Credential Manager-Berechtigungen" auf Seite 531.

Verbindungsprofil-Privilegien

Verbindungsprofil-Privilegien ermöglichen das Erstellen und Ändern von Verbindungsprofilen. Verbindungsprofile speichern die Informationen, die erforderlich sind, um mit Computern und anderen Netzwerkgeräten mit Standard-Netzwerküberwachungsprotokollen zu kommunizieren. Zu diesen Protokollen gehören SNMP, WMI, WSMan und einige andere.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-3 Verbindungsprofil-Privilegien

Recht	Beschreibung
Verbindungsprofil erstellen	Zum Erstellen und Ändern von Verbindungsprofilen.

Verwaltungsrechte

Verwaltungsrechte ermöglichen die Erstellung von Verwaltungselementen wie Filtern, Zielen, Berichten und Aufgaben in der Symantec Management-Plattform.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-4 Verwaltungsprivilegien

Privileg	Beschreibung
Agent-Einstellungen erstellen	Ermöglicht die Erstellung einer neuen Ziel-Agent-Einstellungsrichtlinie bzw. das Klonen einer bestehenden Richtlinie. Die Ziel-Agent-Einstellungen sind die allgemeinen Parameter, die den Symantec Management-Agent steuern, u. a. auch die Kommunikation mit dem Notification Server. Siehe "Konfigurieren der spezifischen Einstellungen" auf Seite 290.
Automatisierungsrichtlinien erstellen	Erlaubt das Erstellen neuer Automatisierungsrichtlinien. Eine Automatisierungsrichtlinie ist dynamisch und legt automatisierte Aktionen zur Durchführung auf dem Notification Server-Computer fest. Die Richtlinie findet die entsprechenden Computer, wenn sie aktiviert wird, und führt die erforderlichen Aktionen basierend auf dem aktuellen Status der einzelnen Zielcomputer aus. Siehe "Infos zu Automatisierungsrichtlinien" auf Seite 408.
Filter erstellen	Erlaubt das Erstellen neuer Ressourcenfilter. Ein Ressourcenfilter, normalerweise einfach als Filter bezeichnet, ist eine dynamische Definition für einen Ressourcensatz. Filter werden mit Organisationsgruppen zur Identifizierung der Ressourcen (Ressourcenziel) verwendet, auf die eine Aufgabe oder Richtlinie angewendet wird. Siehe "Info zu Ressourcenfiltern" auf Seite 369.

Privileg	Beschreibung
Jobs oder Aufgaben erstellen	Ermöglicht die Erstellung von neuen Jobs oder Aufgaben bzw. das Klonen bestehender Jobs oder Aufgaben. Jobs können mehrere Aufgaben, mehrere Jobs und mehrere Bedingungen enthalten, wodurch Sie hohe Flexibilität beim Einrichten der erforderlichen Jobfolge haben. Siehe "Erstellen einer Aufgabe" auf Seite 438. Siehe "Erstellen eines Jobs" auf Seite 439.
Wartungsfenster erstellen	Ermöglicht die Erstellung einer neuen Wartungsfensterrichtlinie bzw. das Klonen einer bestehenden Richtlinie. Ein Wartungsfenster ist die vorgesehene Zeitspanne und Dauer, wenn Wartungsvorgänge auf einem verwalteten Computer ausgeführt werden. Eine Wartungsfensterrichtlinie definiert mindestens ein Wartungsfenster.
Neuen Clientjob erstellen	Hiermit können Sie einen neuen Clientjob erstellen. Clientjobs werden durch einen Task Server auf verwalteten Computern implementiert. Der verwaltete Computer führt anschließend den Job aus und sendet Notification Server eine Rückmeldung. Siehe "Erstellen eines Jobs" auf Seite 439.
Neuen Serverjob erstellen	Hiermit können Sie einen neuen Serverjob erstellen. Serverjobs werden auf Notification Server ausgeführt. Siehe "Erstellen eines Jobs" auf Seite 439.
Organisationsgruppen erstellen	Lässt Sie neue Organisationsübersichten und -gruppen erstellen. Eine Organisationsansicht ist eine hierarchische Ressourcengruppe (genau wie Organisationsgruppen), die einer tatsächlichen Struktur oder Übersicht Ihres Unternehmens entspricht.
Berichte erstellen	Ermöglicht die Erstellung eines neuen Berichts bzw. das Klonen eines bestehenden Berichts. Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.
Ressourcenziele erstellen	Erlaubt das Erstellen neuer Ressourcenziele. Ein Ressourcenziel, normalerweise einfach als Ziel bezeichnet, ist eine Umgebung, in der Aufgaben und Richtlinien auf eine dynamische Ressourcensammlung angewendet werden. Ein Ziel besteht aus mindestens einer Organisationsübersicht oder -gruppe und mehreren Filtern. Die Filter dienen dazu, aus den verfügbaren Ressourcen die benötigten Ressourcen herauszusuchen. Siehe "Info zu Ressourcenzielen" auf Seite 383.
Erkennungsaufgabenverwaltung	Hiermit können Sie Network Discovery-Aufgaben durchführen.

Systemrechte

Die Systemrechte ermöglichen die Ausführung von Verwaltungsaktivitäten wie Sicherheitseinrichtung, Hierarchieverwaltung und Import von XML-Dateien in der Symantec Management-Plattform.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-5 Systemprivilegien

Privileg	Beschreibung
Sicherheit ändern	Sie können die Sicherheitskonfiguration der Symantec Management-Plattform ändern. Sie können Sicherheitsrollen erstellen, Sicherheitsrollen Privilegien und Benutzerkonten zuordnen sowie Berechtigungen für Verwaltungselemente für die einzelnen Rollen zuweisen. Siehe "Einrichten der Sicherheit für die Symantec Management-Plattform" auf Seite 88.
CMDB-Regeln erstellen	Sie können CMDB-Regeln im Daten-Connector erstellen. Mithilfe des Daten-Connectors können Sie Daten zwischen der CMDB und einer Datenquelle übertragen sowie Daten innerhalb der CMDB bearbeiten. Der Daten-Connector ist Teil der erweiterten Symantec Management-Plattform. Siehe "Infos zu Data Connector" auf Seite 495.

Privileg	Beschreibung
SQL direkt bearbeiten	Hiermit können Sie SQL-Abfragen in Berichten und Filtern erstellen oder ändern. Dieses Recht ermöglicht die Bearbeitung einer Datenquellabfrage und die Anzeige von Abfrageergebnisse zu einer "Raw SQL-Abfrage" -Datenquelle für eine Automatisierungsrichtlinie. Wenn ein Benutzer SQL beherrscht und mit der CMDB vertraut ist, kann er sehr spezifische und effiziente Berichte schreiben. Aber auch hier besteht die Möglichkeit zur Umgehung von Sicherheitsprüfungen. Beispielsweise kann ein Benutzer eine Abfrage schreiben, die auf Ressourcen zugreift, die außerhalb ihres Bereichs liegen. Das bedeutet, dass die Ressourcen nicht in den Organisationsgruppen enthalten sind, für die der Benutzer die Berechtigung zum Anzeigen hat. **Warnung:** Schlecht geschriebene SQL-Abfragen können zu falschen Ergebnissen führen, ineffizient sein oder zu viel Speicherplatz und CPU-Zeit auf dem CMDB-Computer verbrauchen. Außerdem kann eine bösartige SQL-Abfrage beliebig Daten in der CMDB löschen, ändern oder hinzufügen. Daher ist dieses Privileg ein hohes Sicherheitsrisiko und wird standardmäßig nur der Rolle "Symantec Administrators" gewährt. Wenn Sie Mitglieder einer Sicherheitsrolle SQL direkt bearbeiten lassen, sollten Sie berichtsbezogene Anwendungs-Identifikationsdaten verwenden, damit die Berichte ein Konto mit eingeschränktem CMDB-Zugriff verwenden müssen. Siehe "Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht" auf Seite 480.
XML importieren/exportieren	Hiermit können Sie Elemente und Ressourcen von speziell strukturierten XML-Dateien importieren und Elemente und Ressourcen in XML-Dateien exportieren. Gehen Sie beim Erstellen von Elementen oder Ressourcen in der Symantec Management-Plattform sorgsam vor, indem Sie in einer XML-Datei gespeicherte Informationen importieren. Bei der Erstellung von Elementen auf diese Weise werden alle Sicherheitsprüfungen umgangen. Beispielsweise kann ein Benutzer einen Bericht erstellen, indem er sein XML importiert, selbst wenn der Benutzer nicht die notwendigen Privilegien bzw. Berechtigungen hat. In diesem Beispiel benötigt der Benutzer das Privileg "Berichte erstellen" sowie die Berechtigung "Untergeordnete Elemente erstellen" für den Ordner, in dem der Bericht gespeichert wird. Dieses Privileg ist ein potenzielles Sicherheitsrisiko. Standardmäßig wird es nur der Rolle "Symantec Administrators" gewährt und sollte Nicht-Administratoren nicht gewährt werden. Siehe "Speichern der Konsolenelemente als XML-Dateien" auf Seite 63.

Privileg	Beschreibung
Daten-Connector verwalten	Hiermit können Sie den Daten-Connector verwalten. Der Daten-Connector ist Teil der erweiterten Symantec Management-Plattform. Mithilfe des Daten-Connectors können Sie Daten zwischen der CMDB und einer Datenquelle übertragen sowie Daten innerhalb der CMDB bearbeiten. Siehe "Infos zu Data Connector" auf Seite 495.
Hierarchiereplikation verwalten	Sie können Hierarchiereplikationsregeln erstellen und ausführen. Die Hierarchiereplikationsregeln legen fest, was auf dem übergeordneten Notification Server sowie auf untergeordneten Notification Servern repliziert wird. Dieses Recht ermöglicht auch den Zugriff auf die Standalone-Replikationsregeln. Siehe "Konfigurieren der Hierarchiereplikation und Hierarchiereplikationsregeln" auf Seite 170.
Hierarchie verwalten	Sie können Ihren Notification Server in eine Hierarchie einfügen oder aus einer Hierarchie entfernen. Sie können Ihren Notification Server in eine Hierarchie als untergeordnetes Element eines bestehenden standortfernen Notification Servers oder als sein übergeordnetes Element einfügen. Denken Sie daran, dass Ihr Notification Server derjenige ist, an dem Sie eingeloggt sind. Dies kann auch ein Remote-Login sein. Um die Hierarchie zwischen zwei Notification Servern zu erstellen oder zu ändern, benötigen Sie dieses Privileg für beide Server.
In Besitz nehmen	Hiermit können Sie eine Sicherheitsentität in Besitz nehmen. Dieses Privileg gewährt dem neuen Besitzer alle Berechtigungen bzgl. der Entität. So würden Sie zum Beispiel den Besitz ergreifen, wenn alle Berechtigungen bzgl. der Entität versehentlich entfernt wurden. Siehe "Besitznahme über Ordner oder Elemente" auf Seite 120.
Sicherheit anzeigen	Ermöglicht die Anzeige der Sicherheitskonfiguration der Symantec Management-Plattform. Diese Informationen enthalten Details zu den Sicherheitsrollen sowie den Benutzerkonten, Privilegien und Berechtigungen, die den einzelnen Rollen zugewiesen sind.

Identifikationsdatenprivilegien

Identifikationsdatenprivilegien ermöglichen das Erstellen neuer Identifikationsdaten im Credential Manager. Credential Manager stellt einen sicheren Speicherort für Benutzernamen und Kennwörter zur Verfügung. Die Typen von Identifikationsdaten, die der Credential Manager speichert, werden durch die auf der Symantec Management-Plattform installierten Lösungen festgelegt.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Wenn Identifikationsdaten erstellt werden, hat nur der Ersteller Zugriff. Wenn andere Benutzer einen Verwaltungsvorgang durchführen müssen, der Identifikationsdaten erfordert, müssen Sie dieses Recht dem entsprechenden Benutzerkonto zuweisen oder der Rolle, die das Benutzerkonto enthält.

Tabelle A-6 Identifikationsdatenprivilegien

Recht	Beschreibung
Identifikationsdaten erstellen	Ermöglicht Ihnen das Erstellen und Ändern von Identifikationsdaten im Credential Manager.

Workflow-Verzeichnisprivilegien

Workflow-Verzeichnisprivilegien ermöglichen das Veröffentlichen von Workflows aus Workflow Designer in Notification Server als Aufgabe oder Elementaktion (eine Option im Kontextmenü).

Workflow Designer ist ein Teil von Workflow Solution. Beim Installieren von Workflow Solution wird der Symantec Management Console eine Seite hinzugefügt, mit deren Hilfe Sie Workflow Designer herunterladen und installieren können. Sie ist nicht standardmäßig in der Symantec Management-Plattform enthalten.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-7 Workflow-Verzeichnisprivilegien

Recht	Beschreibung
Workflows registrieren/Registrierung aufheben	Zum Veröffentlichen von Workflows aus Workflow Designer in Notification Server als Aufgabe oder Elementaktion (eine Option im Kontextmenü). Weitere Informationen finden Sie in der Dokumentation zu Workflow Solution.

Symantec Management Console-Rechte

Mit den Symantec Management Console-Privilegien können Sie die Symantec Management Console anpassen. Diese Privilegien umfassen die Bearbeitung von Menüs sowie die Erstellung von Portalseiten, Web-Parts und Ansichten.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-8 Symantec Management Console-Rechte

Recht	Beschreibung
Portalseiten erstellen	Ermöglicht das Erstellen neuer Portalseiten. Eine Portalseite ist eine Symantec Management Console-Seite, die Sie Ihren Anforderungen entsprechend anpassen können. Sie können eine Portalseite verwenden, um Schlüsselinformationen auf einer einzelnen, überschaubaren Seite zusammenzufassen. Eine Portalseite kann den Status der Symantec Management-Plattform und der verwalteten Computer oder jegliche andere Informationen, die Sie verfügbar machen möchten, anzeigen. Beispielsweise können Sie externe Webseiten, Intranetseiten, RSS-Feeds oder Ihre eigenen Anwendungen einfügen. Sie benötigen hierzu die Berechtigung "Untergeordnete Elemente erstellen" für den Ordner, in dem Sie die neue Portalseite erstellen möchten.
Web-Parts erstellen	Ermöglicht das Erstellen neuer Web-Parts. Web-Parts sind Mini-Webseiten, die Sie als Bausteine für Portalseiten verwenden können. Ein Web-Part kann einen Bericht oder den Inhalt einer Webseite anzeigen. Sie benötigen hierzu die Berechtigung "Untergeordnete Elemente erstellen" für den Ordner, in dem Sie das neue Web-Part erstellen möchten. Siehe "Erstellen und Ändern von Web-Parts" auf Seite 62.
Ansichten erstellen	Ermöglicht das Erstellen neuer Ansichten. Eine Ansicht ist ein Layout mit zwei Teilfenstern mit einer Verzeichnisstruktur im linken Teilfenster und Inhalt im rechten Teilfenster. Die Verzeichnisstruktur enthält Links zu Symantec Management Console-Elementen und ermöglicht es Ihnen, Elemente aus verschiedenen Teilen der Konsole in einer geeigneten Struktur anzuordnen. Ein Element kann mehrmals in einer Ansicht und beliebig oft in verschiedenen Ansichten angezeigt werden. Eine Ansicht kann Ordner, Elementlinks und Weblinks enthalten. Siehe "Info zu Konsolenansichten" auf Seite 35.
Konsolenmenü bearbeiten	Ermöglicht die Anpassung der Menüs in der Symantec Management Console. Die Menüoptionen, die von der Symantec Management-Plattform bereitgestellt werden, sind schreibgeschützt und können nicht geändert werden. Sie können neue Untermenüs hinzufügen und sie bei Bedarf ändern. Sie können jedes Menüelement verschieben oder löschen, ausgenommen diejenigen, die als schreibgeschützt gekennzeichnet sind. Siehe "Anpassen des Konsolenmenüs" auf Seite 54.

Software Management-Rechte

Jedes Software Management -Recht gewährt dem Benutzer bestimmte Rechte zum Ausführen bestimmter Aufgaben in der Ansicht Software und im Fenster Softwarekatalog aus den erweiterten Konsolenansichten. Mit diesen Privilegien können Sie die Softwarebibliothek erstellen sowie Softwareressourcen erstellen und importieren. Diese Software Management -Rechte sind nicht standardmäßig Teil einer Benutzerrolle. Sie müssen das relevante Recht einer Benutzerrolle zuweisen.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-9 Software Management -Rechte

Recht	Beschreibung
"Softwareprodukte erstellen" und "Softwareprodukt-Inventarisierungsfilter definieren"	Mit diesem Recht kann der Benutzer anhand der gespeicherten Suche "Neu erkannte Software" in der Ansicht "Software" neu erkannte Software zu finden. Mit diesem Recht kann der Benutzer die Teilfenster "Neu erkannte bzw. nicht definierte Software" und "Nicht verwaltete Software" im Softwarekatalog verwenden, um Software zu verwalten. Sie müssen dazu der Benutzerrolle die Rechte "Softwareprodukte erstellen" und "Softwareprodukte definieren" zuweisen.
Softwareprodukte erstellen	Mit diesem Recht kann der Benutzer die Schaltfläche "Produkt hinzufügen" verwenden, um das Dialogfeld "Softwareprodukt" zu öffnen. Mit diesem Recht kann der Benutzer außerdem Daten in den Bereichen "Name", "Firma", "Version" und "Kategorie" des Dialogfelds "Softwareprodukt" eingeben. Wenn Sie dieses Recht nicht der Benutzerrolle zuweisen, kann der Benutzer keine Daten in die Bereiche "Name", "Firma", "Version" und "Kategorie" des Dialogfelds "Softwareprodukt" eingeben.
Softwareprodukt-Inventarisierungsfilter definieren	Mit diesem Recht kann der Benutzer auf der Registerkarte "Inventar identifizieren" Softwareprodukt-Inventarisierungsfilter definieren.
Softwarenutzungsverfolgung konfigurieren	Mit diesem Recht kann der Benutzer mit dem Hyperlink "Programmdateien hinzufügen" und der Registerkarte "Nutzung messen/verfolgen" verwenden, um das Softwarenutzungsverfolgung zu konfigurieren.
Softwarelizenzen erstellen	Mit diesem Recht kann der Benutzer über die Schaltfläche "Lizenzen verwalten" Softwarelizenzen erstellen.

Recht	Beschreibung
Softwareressourcen verwalten	Hiermit können Sie Softwareressourcen erstellen, importieren, bearbeiten und löschen. Eine Softwareressource besteht aus den Metadaten, die eine bestimmte Instanz eines Softwareprodukts beschreiben. Eine Softwareressource bietet eine standardisierte Beschreibung der Software, sodass alle softwarebezogenen Aktionen die Software korrekt identifizieren können. Gewöhnlich sollten Sie Softwareressourcen-Privilegien an Benutzerkonten vergeben, die Software verteilen und verwalten. Die Sicherheitsrollen "Symantec-Softwarebibliothekar" und "Asset-Manager" verfügen standardmäßig über dieses Recht.
Softwarebibliothek - Einstellungen verwalten	Hiermit können Sie die "Softwarebibliothekseinstellungen" erstellen und bearbeiten. Die Softwarebibliothek ist der physische Verzeichnisort der Paketdateien, die mit der Software im Softwarekatalog verbunden sind. Weil die Softwarebibliothek ein Repository der endgültigen, autorisierten Versionen der Pakete ist, sollten Sie den Zugriff auf die Bibliothek einschränken, um deren Integrität zu wahren. Die Sicherheitsrollen "Symantec-Softwarebibliothekar" und "Asset-Manager" verfügen standardmäßig über dieses Recht.
Software Delivery erstellen	Hiermit können Sie Softwareverteilungen (Aufgaben "Schnellverteilung" oder "Paketverteilung" und die Richtlinie "Software Delivery verwalten") für ausgewählte Softwareressourcen von der verfügbaren Software-Liste erstellen. Hiermit können Sie die Drag & Drop-Funktion verwenden, um Software Delivery von einer beliebigenSoftware-Liste zu initiieren. Durch diese Berechtigung können Benutzer außerdem die Registerkarte "Delivery" zum Erstellen von Software Deliverys verwenden.

Kontextmenü-Privilegien

Mithilfe der Kontextmenü-Privilegien (auch als Elementaktionen-Privilegien bezeichnet) können Sie allgemeine Aktionen für Elemente in der Symantec Management Console ausführen. Wenn Sie mit der rechten Maustaste auf ein Element klicken, sind die für diesen Elementtyp relevanten Optionen im Kontextmenü verfügbar. Diese Privilegien erlauben das Löschen von Elementen, die Bearbeitung von Ansichten, Weblinks und Elementlinks sowie das Starten, Anhalten und Planen von Aufgaben.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-10 Kontextmenü-Privilegien

Recht	Beschreibung	Gilt für Elementtypen	Zusätzliche Anforderungen
Einer Organisationsgruppe hinzufügen	Ermöglicht das Hinzufügen von Ressourcen zu einer Organisationsgruppe. Siehe "Erstellen und Konfigurieren von Organisationsgruppen" auf Seite 360.	Alle Ressourcen	Schreibberechtigung für die Organisationsgruppe.
Klonen	Sie können ein Element duplizieren.	Alle Elementtypen	Duplizierberechtigung für das Element
Löschen	Lässt Sie ein Element löschen.	Alle Elementtypen	Löschberechtigung für das Element.
Elementverknüpfung bearbeiten	Lässt Sie Elementlinks ändern. Siehe "Info zu Konsolenansichten" auf Seite 35.	Nur Elementlinks.	Schreibberechtigung für den Elementlink.
Regel bearbeiten	Lässt Sie eine Inventarisierungsregel bearbeiten.	Nur Inventarisierungsregeln.	Schreibberechtigung für die Inventarisierungsregel.
Ansicht bearbeiten	Lässt Sie eine Ansicht bearbeiten. Siehe "Erstellen und Ändern von Ansichten" auf Seite 57.	Nur Ansichten	Schreibberechtigung für die Ansicht
Webverknüpfung bearbeiten	Lässt Sie Weblinks ändern. Siehe "Info zu Konsolenansichten" auf Seite 35.	Nur Weblinks.	Schreibberechtigung für den Weblink.
"Zeitplan"	Lässt Sie eine Richtlinie planen. Siehe "Angeben von Richtlinienzeitplänen" auf Seite 404.	Nur Richtlinien.	Schreibberechtigung für die Richtlinie.
Aufgabe planen	Lässt Sie eine Aufgabe planen. Sie können die Aufgabe so einstellen, dass sie zu einem bestimmten Zeitpunkt einmal ausgeführt oder aber regelmäßig wiederholt wird. Siehe "Hinzufügen eines Zeitplans zu einer Richtlinie, einer Aufgabe oder einem Auftrag" auf Seite 444.	Nur Aufgaben.	Berechtigung zum Ausführen der Aufgabe.
Sicherheitsrollenmanager	Sie können den Sicherheitsrollenmanager öffnen.	Alle Elementtypen	Schreibberechtigung für das Element

Recht	Beschreibung	Gilt für Elementtypen	Zusätzliche Anforderungen
Aufgabe starten	Lässt Sie eine Aufgabe sofort starten. Siehe "Ausführen eines Jobs oder einer Aufgabe" auf Seite 442.	Nur Aufgaben.	Berechtigung zum Ausführen der Aufgabe.
Aufgabe anhalten	Lässt Sie eine Aufgabe sofort anhalten.	Nur Aufgaben.	Berechtigung zum Ausführen der Aufgabe.

Kontextmenü: Privilegien für Connector-Beispiele

Privilegien für Connector-Beispiele sind Beispiele für Rechtsklickaktionen durch den Benutzer.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-11 Kontextmenü: Privilegien für Connector-Beispiele

Recht	Beschreibung	Gilt für Elementtypen	Zusätzliche Anforderungen
Computer anpingen	Lässt Sie einen TCP/IP-Ping an einem Computer durchführen.	Nur Computerressourcen	Leseberechtigung für die Organisationsgruppe, die den Computer enthält.

Kontextmenü: Hierarchie-Privilegien

Mithilfe der Hierarchie-Privilegien können Sie die Hierarchiereplikation verwalten. Mithilfe dieser Privilegien können Sie bestimmte Elemente bei der Hierarchiereplikation ein- oder ausschließen sowie Elemente sofort replizieren.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-12 Kontextmenü: Hierarchie-Privilegien

Privileg	Beschreibung	Gilt für Elementtypen	Zusätzliche Anforderungen
Replikation deaktivieren	Hiermit können Sie Elemente aus der Hierarchiereplikation ausschließen. Alle Konfigurations- und Verwaltungselemente sowie Sicherheitsrollen und Privilegien werden standardmäßig repliziert. Diese Option ist nur dann verfügbar, wenn benutzerdefinierte Hierarchiereplikationsregeln verwendet werden. Siehe "Einrichten der benutzerdefinierten Hierarchiereplikation" auf Seite 173.	Alle Elementtypen	Privileg "Hierarchiereplikation verwalten", Schreibberechtigung für das Element.
Jetzt replizieren	Hiermit können Sie ausgewählte Daten direkt von einem Notification Server auf alle untergeordneten Notification Server replizieren, ohne dass sie in eine Replikationsregel eingeschlossen werden müssen. Dieser Replikationsvorgang findet sofort und nur einmal statt. Siehe "Manuelles Replizieren ausgewählter Daten" auf Seite 175.	Alle Elementtypen	Privileg "Hierarchiereplikation verwalten", Schreibberechtigung für das Element.
Replikation aktivieren	Hiermit können Sie Elemente in die Hierarchiereplikation einschließen. Alle Konfigurations- und Verwaltungselemente sowie Sicherheitsrollen und Privilegien werden standardmäßig repliziert. Diese Option ist nur dann verfügbar, wenn benutzerdefinierte Hierarchiereplikationsregeln verwendet werden. Siehe "Einrichten der benutzerdefinierten Hierarchiereplikation" auf Seite 173.	Alle Elementtypen	Privileg "Hierarchiereplikation verwalten", Schreibberechtigung für das Element.

Kontextmenü - Privilegien "Aktionen"

Mit den Privilegien "Aktionen" können Sie Aktionen durchführen, die für Software Management Framework relevant sind. Für zusätzliche Lösungen, die auf der Symantec Management-Plattform installiert werden, können ggf. weitere Privilegien dieser Kategorie hinzugefügt werden.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-13 Kontextmenü - Privilegien "Aktionen"

Privileg	Beschreibung	Gilt für Elementtypen	Zusätzliche Anforderungen
Typ zuordnen	Weist einen Typ einer nicht zugewiesenen Softwareressource im Softwarekatalog zu. Eine nicht zugewiesene Softwareressource ist eine Ressource, die nicht als Softwareversion, -update oder als Service Pack kategorisiert ist.	Nur Softwareressourcen	
Filter für installierte Software erstellen	Erstellt Filter, um verwaltete Computer anhand der installierten Software zu finden.	Nur Softwareressourcen	
Detaillierter Export	Exportiert eine Softwareressource und alle ihre zugeordneten Ressourceninformationen in eine detaillierte XML-Datei.	Nur Softwareressourcen	
Kommandozeile bearbeiten	Öffnet die ausgewählte Kommandozeile zur Bearbeitung innerhalb der Seite zur Bearbeitung der Softwareressource.	Nur Softwareressourcen	
Paket bearbeiten	Öffnet das ausgewählte Paket zur Bearbeitung innerhalb der Seite zur Bearbeitung der Softwareressource.	Nur Softwareressourcen	
Softwareressource bearbeiten	Öffnet die ausgewählte Softwareressource zur Bearbeitung.	Nur Softwareressourcen	
Paket importieren	Ändert die Quelle eines Pakets zur Softwarebibliothek von einer anderen Quelle (z. B. ein Verzeichnis auf dem Server oder ein UNC-Pfad).	Nur Softwareressourcen	
Firmenressource zusammenführen	Führt die ausgewählte Firmenressource mit einer anderen Firmenressource zusammen. Dieses Privileg ist nützlich, wenn Sie zwei Einträge für das gleiche Unternehmen haben, die unter Umständen leicht unterschiedlich geschrieben werden, wie beispielsweise "Symantec" und "Symantec Corporation". Sie können die Elemente auswählen, die zusammengeführt werden sollen, und den entsprechenden Namen angeben, der verwendet werden soll.		

Privileg	Beschreibung	Gilt für Elementtypen	Zusätzliche Anforderungen
Doppelt vorhandene Softwareressourcen auflösen	Wenn zwei Softwareressourcen für die gleiche Software stehen, jedoch verschiedene Kennungen haben, kann der Benutzer in diesem Dialogfeld beide Kennungen einer Softwareressource zuordnen.	Nur Softwareressourcen	

Kontextmenü: Privilegien zum Einstellen des Asset-Status

Mit den Privilegien zum Einstellen des Asset-Status können Sie den Status einer Ressource auf "aktiv" oder "stillgelegt" einstellen.

Lösungen, die auf der Symantec Management-Plattform installiert wurden, fügen dieser Kategorie möglicherweise mehr Privilegien hinzu. Beispielsweise fügt die Asset Management Solution hier drei oder vier Privilegien hinzu.

Siehe "Sicherheitsprivilegkategorien" auf Seite 510.

Siehe "Zuweisen von Privilegien zu einer Sicherheitsrolle" auf Seite 97.

Tabelle A-14 Kontextmenü: Privilegien zum Einstellen des Asset-Status

Privileg	Beschreibung	Gilt für Elementtypen	Zusätzliche Anforderungen
Aktiv	Stellt den Status der ausgewählten Ressource auf "aktiv" ein.	Nur Ressourcen	Schreibberechtigung für die Organisationsgruppe, die die Ressource enthält.
Stillgelegt	Stellt den Status der ausgewählten Ressource auf "stillgelegt" ein.	Nur Ressourcen	Schreibberechtigung für die Organisationsgruppe, die die Ressource enthält.

Ressourcenverwaltungsberechtigungen

Diese Berechtigungen gelten für Ressourcen.

Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.

Tabelle A-15 Ressourcenverwaltungsberechtigungen

Berechtigung	Beschreibung
Ressourcendaten lesen	Sie können Ressourcendaten lesen.
Ressourcenzuordnung lesen	Sie können Ressourcenzuordnungsdaten lesen.
Ressourcendaten schreiben	Sie können Ressourcendaten schreiben.
Ressourcenzuordnung schreiben	Sie können Ressourcenzuordnungsdaten schreiben.

Systemberechtigungen

Diese Berechtigungen, z. B. das Lesen, Schreiben und Löschen von Elementen, gelten für das System.

Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.

Tabelle A-16 Systemberechtigungen

Berechtigung	Beschreibung
Vollständige Kontrolle	Sie können die volle Kontrolle über ein Element übernehmen, das im Besitz eines anderen Benutzers ist. Siehe "Besitznahme über Ordner oder Elemente" auf Seite 120.
Löschen	Sie können Elemente löschen.
Schreiben	Sie können Elemente erstellen oder ändern.
Klonen	Sie können ein vorhandenes Element duplizieren.
Lesen	Sie können ein Element öffnen und den Elementinhalt anzeigen.
Berechtigungen ändern	Sie können die Berechtigungen für Elemente ändern.
Berechtigungen lesen	Sie können die Berechtigungen für ein Element lesen.

Task Server-Berechtigungen

Diese Berechtigungen gelten für Task Server.

Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.

Tabelle A-17 Task Server-Berechtigungen

Berechtigung	Beschreibung
Neue Aufgabe erstellen	Sie können neue Aufgaben erstellen.
Skript ausführen	Sie können ein Skript ausführen.
Energiesteuerung ausführen	Sie können Energiesteuerungsaufgaben ausführen.
Aufgabe ausführen	Sie können Aufgaben ausführen.
'Dienststatus kontrollieren' ausführen	Sie können eine Dienststatuskontrolle ausführen.

Berichtsberechtigungen

Diese Berechtigungen gelten für Berichte.

Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.

Tabelle A-18 Berichtsberechtigungen

Berechtigung	Beschreibung
Berichte ausführen	Sie können einen Bericht ausführen.
Berichte speichern	Sie können einen Bericht speichern.

Richtlinienberechtigungen

Diese Berechtigungen treffen auf Richtlinien zu.

Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.

Tabelle A-19 Richtlinienberechtigungen

Berechtigung	Beschreibung
Zuordnen zu-Ressourcenziel	Lässt Sie Ressourcenziele zu Richtlinien zuordnen.
Richtlinie aktivieren	Lässt Sie eine Richtlinie aktivieren oder deaktivieren.

Ordnerberechtigungen

Diese Berechtigungen gelten für Ordner.

Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.

Tabelle A-20 Ordnerberechtigungen

Berechtigung	Beschreibung
Untergeordnete Elemente erstellen	Sie können Elemente und Unterordner in einen Ordner einfügen.

Filterberechtigungen

Diese Berechtigungen gelten für Filter.

Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.

Tabelle A-21 Filterberechtigungen

Berechtigung	Beschreibung
Agent-Einstellungen anwenden	Sie können die Richtlinie "Spezifische Einstellungen" ändern und auf ein Ressourcenziel anwenden.
Software Delivery-Aufgaben anwenden	Sie können Software Delivery-Aufgaben anwenden.

Verbindungsprofil-Berechtigungen

Diese Berechtigungen ermöglichen die Verwendung von Verbindungsprofilen. Verbindungsprofile speichern die Informationen, die erforderlich sind, um mit Computern und anderen Netzwerkgeräten mit Standard-Netzwerküberwachungsprotokollen zu kommunizieren. Zu diesen Protokollen gehören SNMP, WMI, WSMan und einige andere.

Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.

Verbindungsprofile werden während des Network Discovery-Vorgangs mit Geräten verknüpft. Während der Erkennung wird ein Verbindungsprofil ausgewählt, um die zu verwendenden Protokolle und Identifikationsdaten zu definieren. Wenn die Erkennung abgeschlossen ist, wird dieses Verbindungsprofil mit jeder erkannten Ressource verknüpft. Wenn Informationen erforderlich sind, wird das verknüpfte Verbindungsprofil verwendet, um eine Verbindung herzustellen.

Tabelle A-22 Verbindungsprofil-Berechtigungen

Berechtigung	Beschreibung
Nutzung	Ermöglicht die Verwendung von Verbindungsprofilen.

Credential Manager-Berechtigungen

Credential Manager stellt einen sicheren Speicherort für Benutzernamen und Kennwörter zur Verfügung. Die Typen von Identifikationsdaten, die der Credential Manager speichert, werden durch die auf der Symantec Management-Plattform installierten Lösungen festgelegt. Diese Berechtigungen ermöglichen die Verwendung des Credential Manager.

Siehe "Kategorien von Sicherheitsberechtigungen" auf Seite 512.

Tabelle A-23 Credential Manager-Berechtigungen

Berechtigung	Beschreibung
Nutzung	Ermöglicht die Verwendung des Credential Manager.

Anhang B

Symantec Management Agent

Dieser Anhang enthält folgende Themen:

- Empfohlene Datenaktualisierungsintervalle für den Symantec Management-Agent
- Problemlösungsbefehle für Symantec Management-Agent für UNIX, Linux und Mac

Empfohlene Datenaktualisierungsintervalle für den Symantec Management-Agent

Der Symantec Management-Agent sendet regelmäßig Grundinventardaten an den Notification Server und empfängt Agent-Konfigurationsdaten vom Notification Server. Sie können die Intervalle für diese Aktualisierungen konfigurieren. Je mehr Computer Sie verwalten, desto weniger häufig sollten Sie die Daten aktualisieren, um so die Last des Notification Servers zu reduzieren.

Siehe "Konfigurieren der spezifischen Einstellungen" auf Seite 290.

Tabelle B-1 Empfohlene Symantec Management-Agent-Datenaktualisierungsabstände

Anzahl verwalteter Computer	Grundinventar	Konfigurationsanforderung
0 - 499	30 Minuten	15 Minuten
500 - 1999	8 Stunden	4 Stunden
> 2000	24 Stunden	8 Stunden

Notification Server schließt eine Automatisierungsrichtlinie ein, die Ihnen automatisch eine E-Mail sendet, wenn die Aktualisierungsintervalle niedriger als die empfohlenen Werte sind. Diese Richtlinie, die Skalierbarkeitsprüfung, erspart Ihnen das regelmäßige Prüfen der Aktualisierungsintervalle, wenn Computer Ihrem Netzwerk hinzugefügt oder von ihm entfernt werden. Sie können die Richtlinie zur Skalierbarkeitsprüfung nach Bedarf ein- oder ausschalten und den entsprechenden Zeitplan festlegen.

Siehe "Verwalten von Automatisierungsrichtlinien" auf Seite 410.

Problemlösungsbefehle für Symantec Management-Agent für UNIX, Linux und Mac

Sie können Befehle zur Problemlösung verwenden. Sie müssen sie in einer Eingabeaufforderung auf dem Zielcomputer ausführen. Es sei denn, Sie geben vollständige Pfadnamen an, führen Sie diese Befehle vom lokalen Verzeichnis aus, in dem sich die Binärdatei befindet. Für jeden Befehl wird ein Pfad angegeben.

Hinweis: Das Standardinstallationsverzeichnis für den Symantec Management-Agent ist /opt/altiris/notification/nsagent. Sie können es in der Symantec Management Console unter "Einstellungen > Installationseinstellungen > Agent-Einstellungen" ändern.

Siehe "Installieren von Symantec Management-Agent für UNIX Linux und Mac mit einer manuellen Push-Installation" auf Seite 272.

Tabelle B-2 Symantec Management-Agent-Befehle

Zweck	Befehl aus "/opt/altiris/notification/nsagent/bin"
Erzwingen einer Richtlinienaktualisierung.	`aex-refreshpolicies`
Grundinventar senden.	`aex-sendbasicinv`
Anzeigen verfügbarer Softwarepaketaufgaben mit der Option, sie manuell auszuführen.	`aex-swdapm`
Manuelles Deinstallieren des Agent.	`aex-uninstall`
Neustarten des Agent.	`aex-helper agent restart`

Client Task Agent kann Informationen über alle Aufgaben anzeigen, die dem UNIX-/Linux-Client zugewiesen wurden. Die folgende Tabelle listet nützliche Befehle für Client Task Agent auf.

Tabelle B-3 Client Task Agent-Befehle

Zweck	Führen Sie diesen Befehl aus "/opt/altiris/notification/ctagent/bin" aus.
Anzeigen der Hilfe zu einem Befehl.	`aex-cta help`
Anzeigen aller aktuellen Aufgaben und derer Ausführungsinstanzen.	`aex-cta list`
Auflisten der auf dem Client ausgeführten Aufgaben und ihre GUIDs.	`aex-cta list --show-task-id`
Auflisten ausstehender Aufgaben.	`aex-cta pending`
Aktualisieren der Agent-Konfiguration.	`aex-cta refresh`
Erzwingen einer erneuten Registrierung beim Task Server.	`aex-cta register`
Informationen zum derzeit registrierten Task Server.	`aex-cta ts`
Prüfen, ob der Agent aktiv ist.	`aex-helper check`
Abrufen einer Liste der Richtlinien der kontrollierten Verteilung, die ausgeführt werden.	`aex-cta list`
Abrufen einer Liste der Richtlinien der kontrollierten Verteilung und der Schnellverteilungsaufgaben, die auf dem Client ausgeführt werden.	`aex-cta list --show-all-tasks`
Auflisten von Plugin-Installationsaufgaben.	`aex-smf list`

Zweck	Führen Sie diesen Befehl aus "/opt/altiris/notification/ctagent/bin" aus.
Ermöglichen der Verzögerung der Aufgabenausführung auf dem Client entsprechend der Aufgabeneinstellungen.	`aex-swd-defer`

Tabelle B-4 Software-Verwaltungsbefehle

Zweck	Führen Sie diesen Befehl aus "/opt/altiris/notification/smfagent/bin" aus.
Anzeigen von Software-Verwaltungsaufträgen und deren Status.	`aex-smf list`

Die folgende Tabelle enthält `aex-helper`-Befehle. `aex-helper` ist ein clientseitiges Dienstprogramm zur Problemlösung und Beschleunigen von Administratoraufgaben.

Die Syntax für das Dienstprogramm ist `aex-helper [Befehlsoptionen]`

Tabelle B-5 `aex-helper`-Befehle

Zweck	Befehl aus "/opt/altiris/notification/nsagent/bin"
Registrieren von Abhängigkeiten zwischen Lösungen.	`adddep`
Ausführen verschiedener Aufgaben mit dem UNIX-Agent.	`agent`
Ändern der Eigenschaften von registrierten RC-Diensten.	`changerc`
Prüfen, ob der Symantec Management-Agent für UNIX, Linux und Mac aktiv ist.	`check`
Bereinigen von Elemente aus der XML-Registrierung.	`clean`
Anzeigen der Hilfe zum angegebenen Befehl.	`help`
Abfragen verschiedener Informationen vom Agent.	`info`
Installieren und Registrieren von RC-Skripts.	`installrc`

Zweck	Befehl aus "/opt/altiris/notification/nsagent/bin"
Arbeiten mit dem IPC-Framework des Agent.	`ipc`
Erstellen von Verpackungsskripts und Links für Bibliotheken und Programme.	`Link`
Auflisten von Objekten in der Registrierung des Agent.	`list`
Abfragen verschiedener Informationen vom Agent.	`query`
Starten, Anhalten und Auflisten registrierter RC-Dienste.	`rc`
Hinzufügen eines Objekts zur Registrierung des Agent.	`register`
Deinstallieren von Lösungen.	`uninstall`
Deinstallieren von RC-Skripts.	`uninstallrc`
Entfernen von Verpackungsskripts und Links für Bibliotheken und Programme.	`unlink`
Entfernen von Objekten aus der Registrierung des Agent.	`unregister`
Aktualisieren des Symantec Management-Agent-Plugin	`upgrade`

Sie können auch eine clientseitige Protokolldatei zur Problemlösung verwenden. Verwenden Sie zur Problemlösung anhand dieser Protokolldatei die Befehle in der folgenden Tabelle.

Tabelle B-6 Protokolldateibefehle

Zweck	Befehl aus "/opt/altiris/notification/nsagent/var"
Erhöhen der Protokollierungsstufe auf "Debug".	`aex-helper agent -s Configuration debug_level debug`
Deaktivieren des Protokollgrößen-Limits.	`aex-helper agent -s Configuration debug_file_size 0`

Zweck	Befehl aus "/opt/altiris/notification/nsagent/var"
Wiederherstellen der Standardparameterwerte.	`aex-helper agent -s Configuration debug_level error` `aex-helper agent -s Configuration debug_file_size 1024`

Anhang C

Cloud-fähige Verwaltung - Referenzthemen

Dieser Anhang enthält folgende Themen:

- Kommandozeilenprogramme des Notification Servers
- Unterstützte Konfigurationen für Package Server in einer gemischten Umgebung
- Auswirkungen der Cloud-fähigen Verwaltung auf die Funktionen der Site Server
- Internet-Gateway-Verwaltungsskripts
- Info zur Internet-Gateway-Lastverteilung
- Parameter für Installationspakete Cloud-fähiger Agents
- Kommandozeilen-Switches für Cloud-fähige Agents

Kommandozeilenprogramme des Notification Servers

Die folgende Tabelle enthält Beschreibungen der Kommandozeilenprogramme, die Ihnen auf dem Notification Server zur Verfügung stehen. Sie können diese Programme für die Wartung der Umgebung Ihrer Cloud-fähigen Verwaltung verwenden.

Tabelle C-1 Notification Server-Kommandozeilentools

Name der ausführbaren Datei	Beschreibung
AeXGenClientCert.exe	Mithilfe des Clientzertifikat-Generatortools können Sie die erforderlichen Clientzertifikate erstellen. Die Notification Server-Agent-Zertifizierungsstelle (CA) stellt diese Zertifikate aus. Siehe "Generieren eines temporären Clientzertifikats" auf Seite 343.
AeXGenSiteServerCert.exe	Mithilfe des Serverzertifikat-Generatortools können Sie die erforderlichen Serverzertifikate erstellen. Die Zertifizierungsstelle (CA) des Notification Server stellt diese Zertifikate aus. **Hinweis:** Das Anwenden eines neu generierten Serverzertifikats auf ein Internet-Gateway hat Auswirkungen auf vorhandene Symantec Management-Agents. Die vorhandenen Agents können erst dann eine Verbindung zum Internet-Gateway herstellen, wenn sie aktualisierte Daten des Zertifikatsfingerabdrucks des Gateways erhalten haben. Siehe "Generieren und Anwenden des Site Server-Zertifikats für Zugriff des Cloud-fähigen Agent" auf Seite 309.
AeXRevokeCertificate.exe	Das Zertifikatswiderrufstool. Mithilfe dieses Tools können Sie ein Zertifikat widerrufen, indem Sie die Certificate Revocation List (CRL) aktualisieren. Siehe "Widerrufen eines Zertifikats der Cloud-fähigen Verwaltung" auf Seite 347.

Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Unterstützte Konfigurationen für Package Server in einer gemischten Umgebung

Die IT Management Suite unterstützt eine gemischte Umgebung, in der es sich bei einigen Site Servern um interne und bei einigen um Internet-Site Server handelt. In einer gemischten Umgebung versucht der Symantec Management-Agent die internen Package Server zuerst zu verwenden. Wenn keine internen Package Server verfügbar sind, kehrt der Agent zur Verwendung der Internet-Package Server zurück, die sich hinter einem Gateway befinden.

Tabelle C-2 Unterstützte Konfigurationen für Package Server in einer gemischten Umgebung

Konfiguration	Beschreibung
Definieren Sie einige Internet-Package Server für jede Cloud-fähige Site.	Die Internet-Package Server müssen ihre Codebasen im HTTPS-Format veröffentlichen. Für diese bestimmte Site-Konfiguration können Sie alle Internet-Package Server innerhalb der Site als "uneingeschränkt" kennzeichnen. Diese Konfiguration stellt sicher, dass die Internet-Package Server Pakete nur von bestimmten Internet-Package Servern innerhalb ihrer eigenen Site herunterladen. Wenn ein Internet-Package Server innerhalb der Site ein Paket über das Internet herunterlädt, steht das Paket anderen Internet-Package Servern innerhalb dieser Site zur Verfügung. Dann können die anderen Package Server das Paket vom Package Server herunterladen, der sich in demselben Subnetz befindet, anstatt das Paket im Internet herunterzuladen. Wenn keine internen Package Server der Site zugewiesen werden, muss mindestens ein Internet-Package Server innerhalb der Site verfügbar sein. Diese Konfiguration stellt sicher, dass zumindest ein Package Server Pakete außerhalb seiner Site zur Verteilung innerhalb seiner eigenen Site beziehen kann. Siehe "Konfigurieren eines Package Servers zur Veröffentlichung von HTTPS-Paket-Codebasen" auf Seite 315.
Konfigurieren Sie den Notification Server so, dass er SSL erfordert.	Diese Konfiguration hat zur Folge, dass der Notification Server HTTPS-Codebasen veröffentlicht, wodurch Cloud-fähige Agents und Package Server Pakete vom Notification Server herunterladen können. Dies bedeutet jedoch, dass alle internen (direkt verwalteten) Clients auch mit dem Notification Server unter Verwendung von HTTPS kommunizieren müssten, was möglicherweise nicht wünschenswert ist. Siehe "Konfigurieren des Notification Servers für die Verwendung von HTTPS" auf Seite 304. **Hinweis:** Der Notification Server kann HTTP- und HTTPS-Codebasen nicht gleichzeitig veröffentlichen.

Auswirkungen der Cloud-fähigen Verwaltung auf die Funktionen der Site Server

Die Cloud-fähige Verwaltung hat folgende Auswirkungen auf die Funktionalität von Package Servern und Task Servern:

Tabelle C-3 Auswirkungen der Cloud-fähigen Verwaltung auf die Funktionen der Site Server

Auswirkung	Beschreibung
Package Server im internen Netzwerk stellen Cloud-fähigen Agents und Cloud-fähigen Package Servern Pakete nur über HTTPS bereit.	Jedoch können die Package Server des internen Netzwerks unter Verwendung von UNC oder HTTP weiterhin Pakete auf Clients des internen Netzwerks herunterladen. Auf ähnliche Weise können getrennte Package Server am lokalen Standort unter Verwendung eines beliebigen Protokolls Pakete für Cloud-fähige Clients am selben lokalen Standort bereitstellen.
Das Auswahlverfahren für Server auf Cloud-aktivierten Agents und Package Servern ändert sich.	Das Auswahlverfahren für Server auf internetbasierten Agents und Package Servern sieht wie folgt aus: Die Package Server-Quellen, die dem Cloud-aktivierten Agent oder Package Server zur Verfügung stehen, umfassen lokale Package Server und Package Server des internen Netzwerks. Standardmäßig wählt der Agent von der Liste der lokalen Package Server aus. Der Agent verwendet Package Server des internen Netzwerks nur in den folgenden Szenarien: Alle lokalen Package Server erhalten ein Geschwindigkeitsprofil bei 0 oder mehr als sieben Fehler werden aufgezeichnet.
Zusätzliche Aktivitäten sind erforderlich, wenn Sie einen Package Server löschen.	Wenn Sie einen Package Server von einem Computer löschen, der zum Internet-Gateway hinzugefügt wird, müssen Sie den Package Server aus Sicherheitsgründen auch vom Internet-Gateway löschen.
Ein Remote Task Server kann nicht auf einem Clientcomputer installiert werden, auf dem bereits eine Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" angewendet wird.	Die Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" kann jedoch nach der Installation des Task Servers auf den Clientcomputer angewendet werden.
Task Server können Benachrichtigungen oder Aufgabenverteilungen nicht in Echtzeit bereitstellen.	Periodisches Abrufen ist der unterstützte Modus für das Ausführen von Aufgaben auf Cloud-fähigen Clients. Standardmäßig prüft der Symantec Management-Agent alle 30 Minuten auf Aufgaben. Sie sollten diesen Zeitraum für Cloud-fähige Agents ändern, indem Sie die Einstellung "Aufgabenaktualisierung" in der Richtlinie "Task Agent-Einstellungen" ändern. Sie finden diese Seite mit den Richtlinien in der Symantec Management Console, unter "Einstellungen > Notification Server > Aufgabeneinstellungen". Siehe "Ändern der Client Task Agent-Einstellungen" auf Seite 451.
Der Geschwindigkeitstest für Task Server wird durch zufälliges Sortieren ersetzt.	Der Client Task Agent legt die variable Ausführung der Liste mit Task Servern für Situationen fest, in denen ansonsten die Sortierung auf Basis des Geschwindigkeitstests verwendet werden würde. Beachten Sie, dass der Agent den Geschwindigkeitstest nur ignoriert, wenn er sich im Cloud-fähigen Modus befindet.

Auswirkung	Beschreibung
Standardmäßig funktionieren Task Server sowohl mit Cloud-fähigen als auch mit lokalen Agents.	Task Server, die einer Internetsite zugewiesen sind, funktionieren mit Agents im Intranet und mit Cloud-fähigen Agents. Um zu erzwingen, dass Cloud-aktivierte Agents mit einem ausgewähltem Task Server kommunizieren, müssen Sie diese Agents dem Task Server manuell zuweisen. Siehe "Verwalten manuell zugewiesener Agents" auf Seite 141.

Internet-Gateway-Verwaltungsskripts

Als Hilfsmittel zum Verwalten und Warten Ihrer Internet-Gateways sind im Internet-Gateway-Installationsverzeichnis der Symantec Management-Plattform einige Skripts verfügbar.

Tabelle C-4 Internet-Gateway-Verwaltungsskripts

Speicherort und Name des Skripts	Beschreibung
`Apache\bin\GenerateCert.cmd`	Generiert das Serverzertifikat erneut.
`Apache\certs\Client\UpdateCertHashes.cmd`	Wendet ein Zertifikat der Notification Server-Zertifizierungsstelle (CA) auf das Internet-Gateway an.
`Apache\certs\crl\UpdateCrlHashes.cmd`	Wendet eine Zertifikatsperrliste (CRL) auf das Internet-Gateway an. Siehe "Widerrufen eines Zertifikats der Cloud-fähigen Verwaltung" auf Seite 347.
`Apache\bin\StartService.cmd`	Startet den Internet-Gateway-Dienst.
`Apache\bin\StopService.cmd`	Beendet den Internet-Gateway-Dienst.
`Apache\bin\InstallService.cmd`	Registriert den Internet-Gateway-Dienst in den Windows-Diensten (oder registriert ihn erneut).
`Apache\bin\UninstallService.cmd`	Hebt die Registrierung des Internet-Gateway-Diensts in den Windows-Diensten auf.

Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Info zur Internet-Gateway-Lastverteilung

Das Internet-Gateway kann 3.000 gleichzeitige Verbindungen akzeptieren und unterstützt bis zu 60.000 Endgeräte. Die Höchstzahl von Clients, die ein Internet-Gateway verarbeiten kann, hängt von Ihrer Umgebung ab. Beispiel: Kürzere Richtlinien- und Aufgabeanfragenabstände bedeuten, dass das Gateway mehr Anfragen erhält. Eine höhere Anzahl von Anfragen reduziert die Anzahl von Clients, die das Gateway unterstützen kann. Eine andere Variable ist der Verbindungszeitraum, den die Agents erfordern. In den meisten Fällen stellt der Agent nur für kurze Zeit eine Verbindung her. Wenn der Agent Pakete herunterlädt oder Inventarberichte erstellt, kann eine Verbindung viel länger bestehen.

In der Symantec Management-Plattform werden Internet-Gateways, die Verbindungsprobleme haben, nicht als schlecht gekennzeichnet und ignoriert. Bei jeder Übertragung probiert der Symantec Management-Agent alle Gateways auf seiner Liste aus, bis er ein funktionsfähiges findet. Abhängig von der Art der Probleme, die Gateway-Ausfälle verursachen, besteht die Möglichkeit, dass ein bestimmtes Gateway möglicherweise überlastet wird. Das System sorgt schließlich selbst für das richtige Ausbalancieren ohne manuelles Eingreifen.

Internet-Gateways unterstützen keine manuell konfigurierbare Lastverteilung. Die gesamte Lastverteilung erfolgt automatisch.

Ein Cloud-fähiger Agent führt die Lastverteilung folgendermaßen durch:

- Der Symantec Management-Agent wählt nach dem Zufallsprinzip ein Internet-Gateway aus der Liste der verfügbaren Gateways aus, die in der Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" angegeben sind. Der Agent verwendet dann das ausgewählte Gateway, bis die Verbindung fehlschlägt. Die Auswahl ist immer zufällig, d. h. alle Gateways werden als gleich erachtet und Sie können keinem spezifischen Gateway eine Präferenz oder Gewichtung zuweisen.
- Wenn der Agent keine Verbindung über sein bevorzugtes Gateway herstellen kann, wählt er nach dem Zufallsprinzip ein anderes Gateway aus der Liste. Der Agent verwendet anschließend dieses Gateway für alle Verbindungen, bis es auch fehlschlägt.
- Von Zeit zu Zeit und mit dem doppelten Berichterstellungsabstand für das Grundinventar setzt der Agent seine Auswahl zurück, indem er nach dem Zufallsprinzip ein Gateway aus der Liste der verfügbaren Gateways auswählt.

Dieser Prozess stellt sicher, dass sich die Verbindungslast bald selbst automisch ausbalanciert, wenn ein neues Gateway zum System hinzugefügt wird. Dieselbe automatische Ausbalancierung tritt auf, wenn ein Gateway ein vorübergehendes Problem hat und offline geht.

Siehe "Einrichten der Cloud-fähigen Verwaltung" auf Seite 321.

Siehe "Info zum Vorbereiten des Internet-Gateway-Computers" auf Seite 327.

Parameter für Installationspakete Cloud-fähiger Agents

Sie können ein Symantec Management-Agent-Installationspaket über die Symantec Management Console generieren. Sie müssen das Paket auf der Symantec Management-Plattform-Instanz generieren, die den installierten Agent verwaltet. Das generierte Installationspaket enthält das Symantec Management-Agent-Installationsprogramm für die entsprechende Plattform. Außerdem enthält das Paket die Zertifikate, die der Client benötigt, um den Notification Server als vertrauenswürdig einzustufen.

Wenn Sie ein Agent-Installationspaket generieren, müssen Sie die entsprechenden Paketparameter angeben.

Tabelle C-5 Parameter für Symantec Management-Agent-Installationspakete

Parameter	Beschreibung
Betriebssystem	Das Betriebssystem auf dem Clientcomputer. **Hinweis:** In der Symantec Management-Plattform 7.5 werden nur Microsoft Windows-Clients unterstützt.
Richtlinie	Die Dropdown-Liste enthält alle Richtlinien zur Cloud-fähigen Verwaltung, die derzeit aktiviert sind. Sie müssen die Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" auswählen, die auf diesen Cloud-fähigen Agent angewendet wird. Die ausgewählte Richtlinie gibt die verfügbaren Internet-Gateways an, die der neu installierte Agent verwenden kann. Die Liste der verfügbaren Gateways ist im Symantec Management-Agent-Installationspaket enthalten. Siehe "Konfigurieren der Richtlinie "Einstellungen für die Cloud-fähige Verwaltung" Richtlinie konfigurieren" auf Seite 334.

Parameter	Beschreibung
Organisationsgruppe	Die Organisationsgruppe, zu der der Cloud-fähige Computer gehört. Diese Einstellung ist optional. Wenn Sie eine Organisationsgruppe auswählen, wird der neu installierte Agent automatisch der angegebenen Organisationsgruppe zugewiesen, wenn der Computer in die Verwaltung einbezogen wird. Sie müssen eine Organisationsgruppe verwenden, die Sie erstellt haben. Wählen Sie nicht eine der Standardorganisationsgruppen aus. Diese Gruppen basieren auf Ressourcentypen und sind nicht für Cloud-fähige Computer geeignet. Beispielsweise verwaltet möglicherweise ein Managed Service Provider (MSP) eine Reihe verschiedener Kunden und verwendet für jeden Kunden eine kundenspezifische Organisationsgruppe. Diese Einstellung ermöglicht es, jeden neu installierten Computer automatisch der entsprechenden Organisationsgruppe zuzuweisen.
Installationsname	Ein benutzerfreundlicher Name für das Installationspaket. Dieser Name wird in der Betreffzeile des Symantec Management-Agent-Zertifikats angezeigt, das an das Installationsprogramm angehängt wird. Er kann für Berichts- und Diagnosezwecke genutzt werden. Für eine Einzelcomputerinstallation sollten Sie den Namen des Computers oder des primären Benutzers verwenden. Für ein Paket, das auf mehreren Computern installiert wird, sollten Sie die entsprechende Büro- oder Abteilungskennung verwenden.
Ablaufdatum	Das Datum und die Uhrzeit, zu der das Installationspaket abläuft. Standardmäßig sind es sieben Tage nach der Erstellungszeit. Sie müssen ein Datum angeben, das mindestens einen Tag nach dem aktuellen Datum (Erstellungsdatum) liegt.
Automatische Zertifikatverteilung	Definiert, ob das permanente Zertifikat eines Agents automatisch ausgestellt wird. Wenn es nicht automatisch ausgestellt wird, muss ein Administrator die Zertifikatverteilung verwalten und jede Anforderung aus dem Bereich "Berichte" des Notification Server autorisieren.
Maximalzahl der Agent-Registrierungen	Definiert, wie viele Male ein permanentes Zertifikat ausgestellt werden kann. Das Zertifikat wird basierend auf der Anzahl von Anfragen ausgestellt, die über ein vorübergehendes oder ein Site-Zertifikat gesendet werden.
Signieren mit	Sie haben die Option, dem Installationspaket eine Signatur hinzuzufügen. Sie können zwischen einer Signatur per Kennwort oder Fingerabdruck wählen.

Kommandozeilen-Switches für Cloud-fähige Agents

Sie können Kommandozeilen-Switches verwenden, um den Symantec Management-Agent für die Cloud-fähige Verwaltung zu konfigurieren.

Hinweis: Nachdem Sie Kommandozeilen-Switches verwenden, müssen Sie Symantec den Management-Agent neu starten, damit diese Einstellungen in Kraft treten.

Tabelle C-6 `AeXNSAgent.exe`Kommandozeilen-Switches

Kommandozeilen-Switches	Beschreibung
`/gw-=GatewayName,Port,Fingerabdruck`	Gibt ein Internet-Gateway an, das der Symantec Management-Agent verwenden kann. Siehe "Erzwingen, dass der Symantec Management-Agent ein angegebenes Gateway verwendet" auf Seite 350.
`/importcert=Zertifikatsdatei.pfx`	Fügt der Symantec Management-Agent-Konfiguration ein angegebenes Zertifikat hinzu. Dieser Befehl legt das Zertifikat im Zertifikatspeicher des Symantec Management-Agent-Diensts ab. Außerdem fügt er der Registrierung den Fingerabdruck des Zertifikats hinzu. Siehe "Installieren eines temporären Zertifikats auf einem verwalteten Computer" auf Seite 346.
`/removecert`	Entfernt das aktuelle Zertifikat aus der Symantec Management-Agent-Konfiguration. Dieser Befehl entfernt das Agent-Zertifikat aus dem Zertifikatspeicher des Symantec Management-Agent-Diensts. Außerdem entfernt er den Fingerabdruck des Zertifikats aus der Registrierung. Siehe "Installieren eines temporären Zertifikats auf einem verwalteten Computer" auf Seite 346.
`/rootca=Zertifikatsdatei.cer`	Fügt der Stammzertifizierungsstelle (CA) ein Zertifikat hinzu. Dieser Befehl fügt das angegebene Zertifikat in den Zertifikatspeicher "Vertrauenswürdige Stammzertifizierungsstellen" ein. Siehe "Anwenden eines Zertifikats einer Stammzertifizierungsstelle auf einen verwalteten Computer" auf Seite 305.
`/cem=on`	Aktiviert Cloud-fähige Verwaltung im Symantec Management-Agent durch Aktivieren der sicheren Kommunikation.
`/cem=off`	Deaktiviert Cloud-fähige Verwaltung im Symantec Management-Agent durch Deaktivieren der sicheren Kommunikation.
`/clearcem`	Löscht alle Einstellungen der Cloud-fähigen Verwaltung aus der Konfiguration des Symantec Management-Agent.

Siehe "Fehlerbehebungs- und Wartungsaufgaben der Cloud-fähigen Verwaltung" auf Seite 342.

Anhang D

Benutzerdefinierten Berichtseinstellungen

Dieser Anhang enthält folgende Themen:

- Seite "Benutzerdefinierte Berichte bearbeiten"
- Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle"
- Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrage"
- Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Felder"
- Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Parametrisierte Abfrage"
- Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageparameter"
- Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Filterausdrücke"
- Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Daten-Snapshots"
- Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageauflösung"
- Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Ergebnisse"
- Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Ansichten" für eine Diagrammansicht

- Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Ansichten" für eine Rasteransicht
- Quellfelder bearbeiten Dialogfeld
- "Parameter wird bearbeitet" Dialogfeld

Seite "Benutzerdefinierte Berichte bearbeiten"

Auf der Seite "Benutzerdefinierte Berichte bearbeiten" können Sie die Komponenten und Eigenschaften des von Ihnen erstellten oder bearbeiteten benutzerdefinierten Berichts des Notification Servers festlegen oder bearbeiten.

Siehe "Komponenten eines benutzerdefinierten Notification Server-Berichts" auf Seite 471.

Siehe "Erstellen und Ändern benutzerdefinierter Notification Server-Berichte" auf Seite 473.

Tabelle D-1 Registerkarten auf der Seite "Benutzerdefinierte Berichte bearbeiten"

Registerkarte	Beschreibung
Datenquelle	Hier können Sie eine Berichtsabfrage definieren. Zum Erstellen der Berichtsabfrage können Sie entweder die Abfrage-SQL selbst schreiben oder den Abfragegenerator verwenden. Siehe "Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht" auf Seite 478. Siehe "Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht" auf Seite 480. Siehe "Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle" " auf Seite 550.

Registerkarte	Beschreibung
Ansichten	Hier können Sie Berichtansichten definieren. Die Berichtansicht ist die Art und Weise, wie Berichtergebnisse angezeigt werden. Siehe "Erstellen oder Ändern einer Diagrammansicht für einen benutzerdefinierten Bericht" auf Seite 483. Siehe "Erstellen oder Ändern einer Rasteransicht für einen benutzerdefinierten Bericht" auf Seite 485. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Ansichten" für eine Diagrammansicht" auf Seite 565. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Ansichten" für eine Rasteransicht" auf Seite 568.
Berichtsparameter	Hier können Sie Berichtsparameter und Wertanbieter definieren. Siehe "Definieren von Parametern und Value Providers für einen benutzerdefinierten Bericht" auf Seite 481.
Drilldowns	Hier können Sie Drilldown-Aktionen für einen Bericht einrichten. Siehe "Einrichten der Drilldown-Aktionen für einen benutzerdefinierten Bericht" auf Seite 486.
Erweitert	Hier können Sie die Eigenschaften eines Berichts angeben. Siehe "Festlegen der erweiterten Eigenschaften eines benutzerdefinierten Berichts" auf Seite 489.

Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle"

In der Registerkarte "Datenquelle" können Sie Abfragedetails für einen Notification Server-Bericht (benutzerdefiniert) angeben, den Sie erstellen ändern. Die Ansicht der Registerkarte "Datenquelle" hängt vom Typ der Berichtsabfrage, den Sie definieren, ab und kann die folgenden Registerkarten enthalten:

Thema Ressourcenabfrage	Weitere Informationen finden Sie unter Tabelle D-2.
Thema SQL-Abfrage	Weitere Informationen finden Sie unter Tabelle D-3.

Siehe "Seite "Benutzerdefinierte Berichte bearbeiten"" auf Seite 549.

Siehe "Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht" auf Seite 478.

Siehe "Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht" auf Seite 480.

Wenn Sie eine Ressourcenabfrage bearbeiten, finden Sie auf der Registerkarte "Datenquelle" die Schaltfläche "Diese Abfrage in eine SQL-Abfrage konvertieren". Damit können Sie eine Ressourcenabfrage in eine entsprechende SQL-Abfrage konvertieren. Wenn Sie eine Ressourcenabfrage in eine SQL-Abfrage konvertieren, ändert sich die Ansicht der Registerreiter in der Registerkarte "Datenquelle" automatisch.

Tabelle D-2 Registerreiter auf der Registerkarte "Datenquelle" für eine Ressourcenabfrage

Registerkarte	Beschreibung
Abfrage	Damit können Sie eine Ressourcenabfrage erstellen und die Syntax der Ressourcenabfrage definieren. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrage" " auf Seite 553.
Felder	Damit können Sie Quellfelder zur Verwendung in der Abfrage definieren. Sie können die Datenbanktabelle (Quelle) und Spalte (Feld) auswählen, die Sie aus CMDB extrahieren möchten. Sie können angeben, ob die Quellfelder in den Berichtergebnissen angezeigt werden sollen oder nicht. Sie können auch die Reihenfolge der Spalten und die Zeilenanordnung des Quellfelds im Berichtergebnisraster festlegen. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Felder" " auf Seite 557.
Abfrageparameter	Damit können Sie die Parameter angeben, die in der Abfrage verwendet werden. Dies sind interne Parameter für SQL-Verwendung. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageparameter" " auf Seite 559.

Registerkarte	Beschreibung
Filterausdrücke	Damit können Sie Bedingungsanweisungen erstellen, die zur Verfeinerung der Abfrageergebnisse verwendet werden. Jede Anweisung oder gruppierte Anweisung kann als Filter betrachtet werden. Sie müssen die Anweisungen erstellen, die Sie verwenden möchten, und sie entsprechend gruppieren. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Filterausdrücke" " auf Seite 560.
Abfrageauflösung	Damit können Sie den SQL-Code anzeigen, der auf CMDB ausgeführt wird, um die Berichtergebnisse zu extrahieren. Dieser Code enthält die standardmäßigen Testwerte für alle vom Benutzer angegebenen Parameter. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageauflösung" " auf Seite 563.
Ergebnisse	Damit können Sie die Ergebnisse der Abfrage anzeigen. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Ergebnisse" " auf Seite 564.

Tabelle D-3 Registerreiter auf der Registerkarte "Datenquelle" für eine SQL-Abfrage

Registerkarte	Beschreibung
Parametrisierte Abfrage	Damit können Sie den SQL-Code für die Abfrage schreiben. Dieser Code kann einige Parameter enthalten, die bei Ausführung der Abfrage der CMDB benutzerspezifische Werte übernehmen. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Parametrisierte Abfrage" " auf Seite 558.
Abfrageparameter	Damit können Sie die Parameter angeben, die in der Abfrage verwendet werden. Dies sind interne Parameter für SQL-Verwendung. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageparameter" " auf Seite 559.

Registerkarte	Beschreibung
Daten-Snapshots	Gibt die Bereichsdefinition der GUID-Felder an, die für die Berichtszuordnung der Daten verwendet werden, die von einem Bericht-Snapshot geladen werden. Die Daten werden als Ergebnisse des Berichts angezeigt und entsprechend den Sicherheitsberechtigungen des Benutzers zugeordnet. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Daten-Snapshots" " auf Seite 560.
Abfrageauflösung	Damit können Sie den SQL-Code anzeigen, der auf CMDB ausgeführt wird, um die Berichtergebnisse zu extrahieren. Dieser Code enthält die Standardtestwerte für alle Parameter, die der Benutzer angibt. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageauflösung" " auf Seite 563.
Ergebnisse	Damit können Sie die Ergebnisse der Abfrage anzeigen. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Ergebnisse" " auf Seite 564.

Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrage"

Wenn Sie eine Ressourcenabfrage für einen benutzerdefinierten Bericht oder Filter definieren, müssen Sie eine Ressourcenabfrage auf der Registerkarte "Abfrage" erstellen.

Siehe "Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht" auf Seite 478.

Siehe "Definieren einer Ressourcenabfrage für einen Filter" auf Seite 374.

Auf der Registerkarte "Abfrage" können Sie eine Ressourcenabfrage erstellen. Die Standardvorlage enthält eine Basisabfrage, die alle Ressourcen auswählt. Sie können den Abfragegenerator verwenden, um die Basisabfrage mit den bereitgestellten Bausteinen zu verfeinern. Es sind keine Kenntnisse in SQL-Code erforderlich.

Im linken Fenster des Abfragegenerators wird die Struktur der Abfrage abgebildet. Im rechten Fenster können Sie Objekte in der Abfragestruktur hinzufügen und ändern. Mithilfe des Abfragegenerators können Sie die Abfrage anhand der in der CMDB festgelegten Ressourcenstruktur (Ressourcenklassen, -typen und -verknüpfungen) erstellen. Die Ressourcenabfrage wird im Hintergrund in SQL-Code umgewandelt. Sie können den SQL-Code auf der Registerkarte "Abfrageauflösung" anzeigen.

Tabelle D-4 Optionen auf der Registerkarte "Abfrage" :

Option	Beschreibung
Ressourcentyp	Hier können Sie den Basisressourcentyp ändern. Wurde der Bericht als Computerbericht oder Benutzerbericht erstellt, wird der Basisressourcentyp automatisch auf "Computer" oder "Benutzer" festgelegt.
Alias	Der Alias des Ressourcentyps. Mit dem Alias können Sie einen anderen Namen für den Tabellennamen angeben. Dies ist beispielsweise nützlich, wenn die gleiche Tabelle mehrfach in Verbindungen verwendet wird.
Mit Bereichsfestlegung	Gibt an, ob die Abfrageergebnisse entsprechend der Rolle des Benutzers, der die Abfrage ausführt, in Bereiche unterteilt werden sollen.
Felder & Datenklassenattribute verwenden	Hiermit können Sie der Abfrage Felder hinzufügen. Sie können Felder aus der Datenklasse (z. B. Resource.Name oder Resource.CreatedDate) wählen. Sie können auch Felder aus anderen Tabellen (beispielsweise das Feld "Domäne" aus der Tabelle "Inv_AeX_AC_Identification") auswählen. Auf der Registerkarte "Felder" werden die Felder angezeigt, die im Abfrage-Ergebnissatz definiert sind. Hier können Sie die Darstellung im Ergebnisraster konfigurieren. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Felder" " auf Seite 557.

Option	Beschreibung
Ressourcentypzuordnungen verwenden	Hiermit können Sie der Abfrage Ressourcenzuordnungen hinzufügen. Dies sind vordefinierte Zuordnungen zwischen zwei Typen von Notification Server-Ressourcen (wie z.B. die Computerbenutzerzuordnung, die einen Computer mit einem Benutzer verknüpft). Sie können die Liste von verfügbaren vordefinierten Ressourcentypzuordnungen unter dem Ordner "Einstellungen" im linken Teilfenster anzeigen. Beispie: Klicken Sie auf "Einstellungen" > "Notification Server" > "Einstellungen für Ressourcen und Datenklassen " > "Ressourcenzuordnungen".

Option	Beschreibung
Verbindungen erstellen	Hiermit können Sie der Abfrage Verbindungen hinzufügen. Eine Verbindung kombiniert Datensätze aus zwei verschiedenen CMDB-Tabellen. In der Dropdown-Liste "Verbindungen" können Sie den Verbindungstyp auswählen: ■ Cross Gibt das kartesische Produkt der Datensätze von den zwei verbundenen Tabellen zurück. ■ FullOuter Kombiniert die Ergebnisse der äußeren Verbindungen links und rechts. Die verbundene Tabelle enthält alle Datensätze aus beiden Tabellen und füllt NULL-Werte für alle fehlenden Übereinstimmungen auf der jeweiligen Seite aus. ■ Inner Erfordert, dass jeder Datensatz in den beiden verbundenen Tabellen einen entsprechenden Datensatz hat. ■ LeftOuter Eine Verbindung zwischen zwei Tabellen (A und B). Die verbundene Tabelle enthält immer alle Datensätze der "linken" Tabelle (A), selbst wenn die Verbindungsbedingung keinen entsprechenden Datensatz in der "rechten" Tabelle (B) findet. ■ RightOuter Die Umkehrung der äußeren Verbindung links. Jeder Datensatz aus der "rechten" Tabelle (B) wird zumindest einmal in der verknüpften Tabelle angezeigt. Wählen Sie der nächsten Dropdown-Liste die gewünschte Datenbanktabelle aus. Wählen Sie in der Dropdown-Liste "Ein" die Spalte aus, die verbunden werden soll.
Parameter hinzufügen	Öffnet die Registerkarte "Abfrageparameter", auf der Sie die Parameter angeben können die Sie in der Ressourcenabfrage verwenden möchten. Ein Parameter ist eine Variable, die in die Abfrage übernommen wird. Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageparameter" " auf Seite 559.

Option	Beschreibung
Filterausdrücke hinzufügen	Öffnet die Registerkarte "Filterausdrücke". Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Filterausdrücke" " auf Seite 560.

Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Felder"

Wenn Sie eine Ressourcenabfrage für einen neuen benutzerdefinierten Bericht definieren oder eine Ressourcenabfrage für einen vorhandenen benutzerdefinierten Bericht ändern, können Sie die Quellfelder und Datenklassenattribute angeben, die die Ressourcenabfrage extrahiert.

Auf der Registerkarte "Felder" können Sie die Quellfelder und Datenklassenattribute angeben, die die Ressourcenabfrage extrahiert. Felder sind Spalten aus Tabellen in der CMDB (z. B. die Spalte "Domain" aus der Tabelle Inv_AeX_AC_Identification). Dabei handelt es sich um Datenklassen des von Ihnen ausgewählten Ressourcentyps (z. B. "Computer.Name").

Sie können angeben, ob jedes Quellenfeld in den Berichtergebnissen angezeigt wird. Sie können auch die Reihenfolge der Spalten und die Zeilenanordnung des Quellenfelds im Berichtergebnisraster festlegen.

Siehe "Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht" auf Seite 478.

Siehe "Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle" " auf Seite 550.

Hinweis: Diese Registerkarte wird für nur Berichtsabfragen verwendet. Sie ist für Filterabfragen nicht relevant.

Siehe "Quellfelder bearbeiten Dialogfeld" auf Seite 570.

Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Parametrisierte Abfrage"

Wenn Sie eine SQL-Abfrage für einen neuen benutzerdefinierten Bericht oder Filter definieren, können Sie eine SQL-Abfrage zum Ausführen auf dem CMD schreiben. Wenn Sie eine SQL-Abfrage für einen vorhandenen benutzerdefinierten Bericht oder Filter ändern, können Sie eine SQL-Abfrage zum Ausführen auf dem CMD schreiben. Auf der Registerkarte "Parameterisierte Abfrage" können Sie die SQL-Abfrage schreiben, die auf die CMDB ausgeführt werden soll. Diese Registerkarte enthält ein Textfeld, in dem Sie den SQL-Code eingeben oder aus der Zwischenablage einfügen können. Im Fenster "Objekt-Explorer" können Sie Quellfelder aus der CMDB auswählen und in die Abfrage einfügen. Das Einsetzen der Quellfelder vereinfacht das Schreiben der Abfrage.

Siehe "Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht" auf Seite 480.

Sie benötigen die Berechtigung zum Bearbeiten von SQL, um SQL-Abfragen zu erstellen oder zu ändern. Zudem sollten Sie sich mit der CMDB-Tabellenstruktur auskennen. Sollen Bereiche auf die Abfrageergebnisse angewendet werden, müssen Sie den entsprechenden SQL-Code in die Abfrage einfügen.

Siehe "Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle" " auf Seite 550.

Tabelle D-5 Optionen auf der Registerkarte "Parametrisierte Abfrage"

Option	Beschreibung
Textfeld	Hier können Sie die SQL-Abfrage eingeben. Sie können den SQL-Code komplett neu eingeben oder aus der Zwischenablage einfügen. Wenn Sie ein Quellfeld in die SQL-Abfrage aufnehmen möchten, klicken Sie an der gewünschten Stelle in den SQL-Code und dann in der Zeile "Objekt" bzw. "Feld" auf "Hinzufügen".
Objekt	Wählen Sie hier die gewünschte Datenbanktabelle aus.
Feld	Wählen Sie hier die gewünschte Tabellenspalte aus.
Alias	Geben Sie hier die Aliasnamen für die Datenbanktabelle und die Tabellenspalte ein.

Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageparameter"

Wenn Sie eine Abfrage für einen neuen benutzerdefinierten Bericht oder einen Filter definieren oder eine Abfrage für einen vorhandenen benutzerdefinierten Bericht oder einen Filter ändern, können Sie Abfrageparameter verwenden. Auf der Registerkarte "Abfrageparameter" können Sie die Parameter angeben, die Sie in der Berichts- oder Filterabfrage verwenden möchten. Ein Parameter ist eine Variable, die in der Abfrage enthalten ist. Parameterwerte für Filter- und Berichtsabfragen sind unter Umständen systemdefiniert oder aus einem anderen Bericht extrahiert. Nur für Berichtsabfragen kann ein Benutzer die entsprechenden Parameterwerte auf der Seite "Bericht" festlegen. Wenn die Abfrage ausgeführt wird, werden die angegebenen Parameterwerte im SQL-Code verwendet.

Siehe "Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht" auf Seite 478.

Siehe "Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht" auf Seite 480.

Siehe "Definieren einer Ressourcenabfrage für einen Filter" auf Seite 374.

Siehe "Definieren einer SQL-Abfrage für einen Filter" auf Seite 377.

Durch Verwenden von Parametern in Abfragen können Sie eine flexible Abfrage erstellen. Sie können solch eine Abfrage verwenden, um verschiedene Ergebnisse zu extrahieren, indem Sie die entsprechenden Parameterwerte einfügen. Beispielsweise können Sie eine Abfrage erstellen, die Parameter für den Computersystemtyp und den Betriebssystemnamen enthält. Sie können diese Abfrage für jede gültige Kombination aus Systemtyp/Betriebssystemname ausführen, um die gewünschten Ergebnisse zu extrahieren. Sie können die Parameterwerte in der Abfrage auch als Hard Code festlegen. Sie würden dann die Abfrage jedes Mal ändern, wenn Sie eine andere Kombination aus Systemtyp/Betriebssystemname hätten verwenden wollen. Sie können auch mehrere Abfragen mit einer anderen in jeder Abfrage definierten Kombination aus Systemtyp/Betriebssystemname erstellen.

Wenn Sie einen Parameter auf der Registerkarte "Abfrageparameter" erstellen, wird die entsprechende Parametererklärung automatisch einer Ressourcenabfrage hinzugefügt. Wenn Sie jedoch eine SQL-Abfrage schreiben, müssen Sie die entsprechende Parametererklärung dem Abfragecode manuell hinzufügen.

Wenn Sie einen Parameter in einer Berichtsabfrage einschließen, können Sie den Value Provider für den Parameter einrichten. Sie können den Value Provider-Typ und die gültigen Werte für den Parameter angeben. Anhand des Value Providers

kann der Benutzer im Allgemeinen den entsprechenden Parameterwert bei Ausführung des Berichts festlegen. Sie legen den Value Provider für einen Parameter auf der Registerkarte "Berichtsparameter" fest.

Siehe "Definieren von Parametern und Value Providers für einen benutzerdefinierten Bericht" auf Seite 481.

Siehe "Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle" " auf Seite 550.

Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Filterausdrücke"

Wenn Sie eine Abfrage für einen neuen benutzerdefinierten Bericht oder Filter definieren oder eine Abfrage für einen vorhandenen benutzerdefinierten Bericht oder einen Filter ändern, können Sie Filterausdrücke einrichten, um die Abfrageergebnisse zu verfeinern. Auf der Registerkarte "Filterausdrücke" können Sie Regeln zum Verfeinern der Abfrageergebnisse angeben. Bei diesen Regeln handelt es sich um Bedingungsanweisungen, mit denen die groben Ergebnisse der Abfrage gefiltert werden, um die gewünschten Ressourcen zu ermitteln.

Siehe "Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht" auf Seite 478.

Siehe "Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle" " auf Seite 550.

Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Daten-Snapshots"

Diese Informationen sind nur für Berichtsabfragen relevant. Die Registerkarte "Daten-Snapshots" wird nicht in den Filterabfragen angezeigt.

Sie können die Bereichsdefinitionsfelder in einer SQL-Abfrage angeben, um sicherzustellen, dass die erfassten Bericht-Snapshots richtig bewertet werden können, wenn anderer Benutzer darauf zugreifen. Felder für die Bereichsdefinition sind die GUID-Felder, die für die Bereichsdefinition der aus einem Bericht-Snapshot extrahierten Daten verwendet werden. Wenn der Benutzer auf einen Bericht-Snapshot zugreift, werden die Daten entsprechend den Sicherheitsberechtigungen des Benutzers aus dem Snapshot geladen. Wenn ein

Feld keine Bereichsdefinition aufweist, werden alle relevanten Elemente geladen. Wenn ein Feld eine Bereichsdefinition aufweist, werden nur diejenigen Elemente geladen, für die der Benutzer, der die Daten anzeigt, eine Leseberechtigung hat.

Siehe "Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht" auf Seite 480.

Die Bereichsdefinitionsfelder, die Sie auf der Registerkarte "Daten-Snapshots" konfiguriert haben, beziehen sich nur auf das Extrahieren von Daten aus Bericht-Snapshots. Sie beeinflussen nicht die SQL-Abfrage, die Daten aus CMDB extrahiert, um sie als Bericht-Snapshot zu speichern. Zur Festlegung einer Bereichsdefinition für eine SQL-Abfrage müssen Sie den passenden SQL-Code einschließen, um Ergebnisse entsprechend der Sicherheitsberechtigungen des Benutzers zu extrahieren, der die Abfrage ausführt.

Hinweis: Wenn eine SQL-Abfrage eine Bereichsdefinition aufweist, werden alle Bericht-Snapshots mit dem Bereich des Benutzers gespeichert, der die Abfrage ausgeführt hat. Wenn ein Snapshot gemeinsam genutzt werden soll, stellen Sie sicher, dass er alle Daten enthält, die für andere Benutzer relevant sein können. Sie können dazu die Berichtsabfrage als ein Benutzer ausführen, der Zugriff auf alle Ressourcen hat (z. B. ein Mitglied der Rolle "Symantec-Administrator"). Sie können auch eine geplante Aufgabe "Bericht ausführen" verwenden, um den passenden Snapshot zu erstellen: Standardmäßig wird die Aufgabe im Administratorkontext ausgeführt. Somit wird der Snapshot mit einem globalen Definitionsbereich erfasst.

Standardmäßig ist in neuen SQL-Berichten `[_ItemGuid]` als ein GUID-Feld mit Bereichsdefinition konfiguriert. Dieses Feld wird verwendet, um für die Ergebnisse mit einer Verbindung zu einer Bereichsdefinitionsfunktion den Bereich wie folgt festzulegen:

```
INNER JOIN [fnGetTrusteeScopedResources](@v1_TrusteeScope) AS [fnGTSR]

   ON ([vri2_Resource].[Guid] = [fnGTSR_3].[ResourceGuid])
```

Dabei ist `[vri2_Resource].[Guid]` der vollständige Name des Felds mit dem Alias `[_ItemGuid]`.

Siehe "Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle" " auf Seite 550.

Tabelle D-6 Optionen auf der Registerkarte "Daten-Snapshots"

Option	Beschreibung
Bereichsdefinition der Felder	Hier können Sie alle in der SQL-Abfrage enthaltenen GUID-Felder anzeigen. Sie müssen die GUID-Felder angeben, die für die Bereichsdefinition verwendet werden. Wenn Sie eine komplexe SQL-Abfrage erstellen, die mehrere Verbindungen zu Ressourcen und mehrere Anwendungen für die Bereichsdefinitionsfunktion aufweist, sollten Sie alle passende Bereichsdefinitions-GUIDs der Liste "Bereichsdefinition der GUID-Felder" hinzufügen.
Daten-Snapshot-Abfrage	Hier können Sie den SQL-Code anzeigen, der erzeugt wird, wenn der Snapshot gespeichert oder geladen werden muss. Bevor Sie die Berichtsabfrage speichern, können Sie überprüfen, ob der SQL-Code zum Laden von Snapshot-Daten die Bereichsdefinition richtig auf die gespeicherten Ergebnisse anwendet. Die Abfrage im Textfeld wird automatisch aktualisiert, wenn Sie die Bereichsdefinitionsfelder oder die Auswahl in der Dropdown-Liste "Daten-Snapshot-Abfragemodus" ändern. Wird sie nicht automatisch aktualisiert, klicken Sie auf "Aktualisieren", um den angezeigten SQL-Code zu aktualisieren.

Option	Beschreibung
Daten-Snapshot-Abfragemodus	Hier können Sie den Abfragemodus auswählen: ■ Tabelle mit Snapshot-Daten erstellen Zeigt den SQL-Code an, der die Tabellenstruktur der Snapshot-Daten erstellt. Diese Struktur hängt nicht von der Konfiguration der Bereichsdefinition ab. ■ Snapshot-Daten speichern Zeigt den SQL-Code an, der Daten für alle Felder in der Snapshot-Datentabelle speichert. Die Bereichsdefinitionskonfiguration hat keinen Einfluss auf diese Daten. ■ Snapshot-Daten laden Zeigt den SQL-Code an, der Daten aus der Snapshot-Datentabelle lädt und entsprechend den Sicherheitsberechtigungen des Benutzers ihre Bereichsdefinition festlegt. SQL verwendet die konfigurierten Bereichsdefinitionsfelder und die TrusteeScope-Mitgliedschaft des Benutzers, um die passenden Daten zu extrahieren. Diese Daten werden dann dem Benutzer als Berichtergebnisse vorgelegt. Die angegebene Bereichsdefinitionsfelder definieren den Bereich dieser Daten.

Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Abfrageauflösung"

Sie können die aufgelöste Abfrage eines von Ihnen erstellten oder geänderten benutzerdefinierten Berichts oder Filters anzeigen. Die Registerkarte "Abfrageauflösung" zeigt den SQL-Code an, der auf dem CMDB ausgeführt wird. Alle Parameter, die Sie angegeben haben, werden auf die entsprechenden Prüfwerte eingestellt.

Siehe "Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht" auf Seite 478.

Siehe "Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht" auf Seite 480.

Wenn Sie eine Ressourcenabfrage anzeigen, können Sie den Abfragemodus in der Dropdown-Liste "Ressourcenabfragemodus" auswählen:

Normal	Zeigt die Standardabfrageauflösung an. Die Standardabfrageauflösung wird anhand der Ressourcenabfrage erstellt, die Sie im Abfragegenerator angegeben haben.
Tabelle mit Snapshot-Daten erstellen	Ergänzt die Abfrage mit SQL-Code, um eine Snapshot-Datentabelle für die Abfrageergebnisse zu erstellen. Die geänderte Abfrage wird angezeigt.
Snapshot-Daten speichern	Ergänzt die Abfrage mit SQL-Code, um die Abfrageergebnisse in einer Snapshot-Datentabelle zu speichern. Die geänderte Abfrage wird angezeigt.
Snapshot-Daten laden	Ergänzt die Abfrage mit SQL-Code, der die Abfrageergebnisse aus einer Snapshot-Datentabelle anstatt der CMDB extrahiert. Die geänderte Abfrage wird angezeigt.

Siehe "Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle" " auf Seite 550.

Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Ergebnisse"

Sie können die Ergebnisse einer benutzerdefinierten Berichtsabfrage auf der Registerkarte "Ergebnisse" anzeigen. Wenn Sie die Registerkarte "Ergebnisse" öffnen, wird die Abfrage automatisch in der CMDB ausgeführt und die aktuellen Ergebnisse werden angezeigt. Sie können Änderungen an der Abfrage überprüfen und verschiedene Einstellungen für die Abfrageparameter testen.

Siehe "Definieren einer Ressourcenabfrage für einen benutzerdefinierten Bericht" auf Seite 478.

Siehe "Definieren einer SQL-Abfrage für einen benutzerdefinierten Bericht" auf Seite 480.

Siehe "Seite zum Bearbeiten benutzerdefinierter Berichte: Registerkarte "Datenquelle" " auf Seite 550.

Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Ansichten" für eine Diagrammansicht

Auf der Registerkarte "Ansichten" für eine Diagrammansicht können Sie auf den folgenden Unterregisterkarten Einstellungen angeben:

Titel	Geben Sie hier den Diagrammtitel und dessen Position an. Siehe Tabelle D-7 auf Seite 566.
Legende	Geben Sie hier die Legende und deren Position an. Die Legende ist eine optionale Beschreibung, die im Diagramm angezeigt wird. Siehe Tabelle D-8 auf Seite 566.
3D	Durch Einrichten des 3D-Zooms können Sie ausgewählte Bereiche des Diagramms auf die volle Fenstergröße vergrößern. Beispielsweise empfiehlt es sich, einen Drilldown für einen großen Bericht durchzuführen, der einen langen Zeitraum umfasst: Sie können einen bestimmten kurzen Zeitraum anzeigen, indem Sie den relevanten Teil auswählen. Sie können eine oder beide Achsen als "erweiterbar" festlegen. Siehe Tabelle D-9 auf Seite 567.
X-Achse	Wählen Sie hier die Ergebnisspalte aus, die als X-Achse im Diagramm verwendet werden soll. Außerdem können Sie den Titel angeben und die Darstellung der X-Achse einrichten. Siehe Tabelle D-10 auf Seite 567.
Y-Achse	Hier können Sie die Ergebnisspalte (bzw. -spalten) angeben, die als Y-Achse im Diagramm verwendet werden soll/en. Außerdem können Sie den Titel angeben und die Darstellung der Y-Achse einrichten. Bei einigen Diagrammtypen können Sie mehrere Werte (mehrere Ergebnisspalten) im gleichen Diagramm stapeln. Diese werden als mehrere Zeilen in einem Liniendigramm oder als Stapel mit verschiedenen Farben in einem Balkendiagramm jeweils farbcodiert und gekennzeichnet angezeigt. Siehe Tabelle D-11 auf Seite 567.

Siehe "Erstellen oder Ändern einer Diagrammansicht für einen benutzerdefinierten Bericht" auf Seite 483.

Tabelle D-7 Optionen auf der Registerkarte "Titel"

Option	Beschreibung
Titel	Der Name des Diagramms. Wenn Sie einen mehrzeiligen Titel wünschen, verwenden Sie die Eingabe **\n**, um an den gewünschten Stellen Zeilenumbrüche vorzunehmen. Standardmäßig wird kein Name vorgegeben. Der Titel ist daher immer leer.
QuickInfo	Der Text, der in der QuickInfo erscheint, die beim Bewegen der Maus über den Diagrammtitel angezeigt wird. Es ist keine Standardvorgabe festgelegt.
Ausgerichtet	Geben Sie hier die Position und die Ausrichtung des Texts relativ zum Diagramm für die Systemsprache an (schriftliches Format).
Docking	Geben Sie hier die Position des Titels auf der Diagrammseite an.

Tabelle D-8 Optionen auf der Registerkarte "Legende"

Option	Beschreibung
Legende anzeigen	Aktivieren Sie diese Option, damit die Legende angezeigt wird.
In Zeichnungsfläche	Aktivieren Sie diese Option, damit die Legende innerhalb der Zeichnungsfläche angezeigt wird. Wenn diese Option deaktiviert wird, erscheint die Legende außerhalb der Zeichnungsfläche.
Titel	Der Legendentext. Es wurde keine Standardeinstellung festgelegt, somit ist die Standardlegende eine leere Zeichenfolge.
Stil	Geben Sie hier den Legendenstil an.
Ausgerichtet	Geben Sie hier die Ausrichtung des Legendentextes relativ zum Diagramm an.

Option	Beschreibung
Docking	Geben Sie hier die Position der Legende auf der Diagrammseite an.

Tabelle D-9 Optionen auf der Registerkarte "3D"

Option	Beschreibung
3D aktivieren	Aktivieren Sie diese Option, um den 3D-Zoom zu aktivieren.
Zoom	Aktivieren Sie diese Option, um Zoom für die X- bzw. Y-Achse zu aktivieren.
"Drehung"	Der Drehwinkel um die X- bzw. Y-Achse.

Tabelle D-10 Optionen auf der Registerkarte "X-Achse"

Option	Beschreibung
Hauptspalte	Die Datenspalte, die entlang der X-Achse dargestellt werden soll. Wählen Sie die entsprechende Option aus der Dropdown-Liste aus. Die Optionen sind die Ergebnisspalten, die im Bericht angegeben wurden.
Titel	Der Text für die X-Achse.
Sichtbar	Aktivieren Sie diese Option, um die X-Achse anzuzeigen.
Hauptraster	Aktivieren Sie diese Option, um die Hauptrasterlinien der X-Achse anzuzeigen.
Umgekehrt	Aktivieren Sie diese Option, die X-Achse in umgekehrter Reihenfolge darzustellen.

Tabelle D-11 Optionen auf der Registerkarte "Y-Achse"

Option	Beschreibung
Hauptspalte	Die Datenspalte, die entlang der Y-Achse dargestellt werden soll. Wählen Sie die entsprechende Option aus der Dropdown-Liste aus. Die Optionen sind die Ergebnisspalten, die im Bericht angegeben wurden.
Titel	Der Text für die Y-Achse.

Option	Beschreibung
Gestapelte Spalten	Die Liste der Spalten, die zur Verfügung stehen, um dem Diagramm hinzugefügt zu werden. Wählen Sie die Spalten aus, die Sie hinzufügen möchten. Diese Option gilt nur für gestapelte Diagrammtypen, wie beispielsweise "Gestapelte Spalte", "Gestapelter Balken" und "Gestapelte Fläche".
Sichtbar	Aktivieren Sie diese Option, um die Y-Achse anzuzeigen. Standardmäßig ist diese Option deaktiviert und die Y-Achse wird nicht angezeigt.
Hauptraster	Aktivieren Sie diese Option, um die Hauptrasterlinien der Y-Achse anzuzeigen. Standardmäßig ist diese Option deaktiviert und die Hauptrasterlinien der Y-Achse sind nicht sichtbar.
Umgekehrt	Aktivieren Sie diese Option, um die Y-Achse in umgekehrter Reihenfolge darzustellen. Standardmäßig ist diese Option deaktiviert.

Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Ansichten" für eine Rasteransicht

Auf der Registerkarte "Erweiterte Formatierung" können Sie die erweiterte Formatierung für die Rasteransicht eines benutzerdefinierten Berichts einrichten.

Beim Einrichten der erweiterten Formatierung werden Formatierungsregeln für die entsprechenden Ergebnisspalten erstellt. Für jede Formatierungsregel muss die HTML-Kennzeichnung angegeben werden, die mithilfe der Regel auf die Ergebnisse angewendet wird. Wenn die Formatierungsregel für einige Datenwerte Bedingungen enthält, müssen entsprechende Bedingungen angegeben werden. Nehmen Sie an, in einem Computerbericht über den Festplattenspeicher soll die Formatierungsregel nur für Computer gelten, die über weniger Speicherplatz als das festgelegte Minimum verfügen. In diesem Fall enthält die Regel eine Bedingung, dass der freie Speicherplatz unterhalb des angegebenen Minimums liegen muss.

Siehe "Erstellen oder Ändern einer Rasteransicht für einen benutzerdefinierten Bericht" auf Seite 485.

Tabelle D-12 Optionen auf der Registerkarte "Erweiterte Formatierung" :

Option	Beschreibung
Regelname	Geben Sie hier den Regelnamen an.
"Formattyp"	Geben Sie hier den Formattyp des Berichts an.
Gilt für	Geben Sie hier an, ob die HTML-Formatierung in der Vorlage für die gesamte Rasterzeile oder nur die ausgewählte Spalte gelten soll. Alle Datenspalten aus den Berichtergebnissen werden aufgeführt. Wenn die Berichtergebnisse Elemente enthalten, ist auch die Spalte "Element-GUID" verfügbar. Diese Spalte wird in allen Ansichten ausgeblendet, ist aber in den Abfrageergebnissen enthalten.
Bedingung:	Sie können Bedingungsanweisungen innerhalb der Formatierungs-Regeln festlegen, um die Regeln nur auf bestimmte Datenwerte anzuwenden. Beispielsweise empfiehlt es sich, bestimmte Datenwerte im Raster zu markieren, oder fehlende Datenwerte zu identifizieren. Wenn Sie Bedingungen für die Formatierungsregel festlegen möchten, aktivieren Sie die Option "Bedingung". Unter "Bedingung" können Sie Bedingungen für die Formatierungsregel festlegen: ■ Spalte Gibt die Spalte an, für die die Bedingung gilt. Jede Daten-Spalte in den Berichtergebnissen wird aufgelistet. ■ Prüfen Der Bedingungsoperator. ■ "Wert" und "Wert 2" Gibt den Wert oder die Werte an, der/die zum Prüfen der Bedingung verwendet wird/werden.
Format	Richten Sie hier die Felder für die Formatierungsvorlage ein: ■ Quellwert Gibt die Quelle der Daten an, die in der formatierten Zelle angezeigt werden. Der Standard ist "Angewandter Wert" (der in der Zelle vorgegebene Wert). Auf Wunsch können Sie diesen Wert jedoch durch einen beliebigen anderen aus der gleichen Zeile ersetzen. Jede Daten-Spalte in den Berichtergebnissen wird aufgelistet. ■ Quelltyp Der anzuzeigende Quelltyp.

Quellfelder bearbeiten Dialogfeld

Im Dialogfeld "Quellfelder bearbeiten" können Sie die Einstellungen für die Quellfelder in Ihrer Ressourcenabfrage ändern.

Siehe "Seite zum Bearbeiten von benutzerdefinierten Berichten: Registerkarte "Datenquelle" : Registerkarte "Felder" " auf Seite 557.

Tabelle D-13 Einstellungen im Dialogfeld "Quellfelder bearbeiten"

Einstellung	Beschreibung
Alias	Der Feld-Alias. Es empfiehlt sich, einen Feld-Alias anzugeben, um das rohe SQL (angezeigt auf der Registerkarte "Abfrageauflösung") lesbarer und verständlicher zu machen.
Auswählen	Legt fest, ob das Feld in den Abfrageergebnissen eingeschlossen wird. Standardmäßig werden alle Felder ausgewählt.
Sichtbar	Legt fest, ob das Feld in den Berichtergebnissen angezeigt wird, die für den Benutzer sichtbar sind. Standardmäßig sind alle Felder sichtbar. Sie können diese Option verwenden, um bestimmte Felder für den Benutzer unsichtbar zu machen. Beispielsweise soll die Abfrage bestimmte Informationen extrahieren, beispielsweise eine Computer-GUID, die für den Benutzer nicht relevant, jedoch für andere Zwecke nützlich ist. Die Daten werden trotzdem als Teil der Abfrageergebnisse extrahiert und eventuell von Automatisierungsrichtlinien verwendet.
Spaltenreihenfolge	Legt die Reihenfolge der Spalten im Berichtergebnisraster fest. Die Spalten werden von links nach rechts nummeriert.
Sortierrichtung	Ermöglicht es, die Sortierrichtung im Berichtergebnisraster anzugeben.

Einstellung	Beschreibung
Sortierreihenfolge	Legt die Sortierreihenfolge dieser Spalte im Berichtergebnisraster fest. Die Sortierreihenfolge wird mit der angegebenen Sortierrichtung verwendet. Wenn Sie Quellfelder für eine Ressourcenabfrage in einem Bericht oder Filter angeben, wird die Sortierreihenfolge angepasst, sobald Sie die Sortierrichtung ändern. Wenn Sie die Sortierungsreihenfolge eines Felds in die eines anderen ändern, wird das geänderte Feld ensprechend sortiert. Die anderen Felder werden entsprechend neu angeordnet. Um das Sortieren zu entfernen, setzen Sie die Sortierreihenfolge auf N/V (nicht verfügbar) zurück. Die Sortierrichtung wird automatisch auf "Standard" zurückgesetzt und die Sortierreihenfolge der anderen Felder wird entsprechend angepasst, um alle Lücken zu füllen.
Aggregat	Ermöglicht es anzugeben, wie man die Werte in dieser Spalte im Berichtergebnisraster bündelt.
Gruppenreihenfolge	Gibt die Sortierreihenfolge der gebündelten Zeilen an.
Bereichsdefinition	Gibt an, ob das Feld in den Abfrageergebnissen eine Bereichsdefinition haben soll. Standardmäßig unterliegen die Felder keiner Bereichsdefinition. Das heißt, die Abfrage extrahiert alle relevanten Elemente. Wenn das Feld eine Bereichsdefinition hat, extrahiert die Abfrage nur die Elemente, für die der Benutzer, der die Abfrage ausführt, eine Leseberechtigung hat. **Hinweis:** Die Abfrageergebnisse, die der Benutzer als Berichtergebnisse anzeigt, oder die Filtermitgliedschaft unterliegen stets einer Bereichsdefinition, die durch die Benutzerrolle bestimmt ist. Die Bereichsdefinition wird automatisch angewendet, wenn die Abfrageergebnisse dem Benutzer vorgelegt werden. Das Ändern der Einstellung hat keine Wirkung auf das, was der Benutzer anzeigen kann.

"Parameter wird bearbeitet" Dialogfeld

Das Dialogfeld "Parameter wird bearbeitet" ermöglicht es, die Parametereinstellungen für alle Parameter des benutzerdefinierten Berichts anzugeben. Unter "Parameter" können Sie die allgemeinen Parametereinstellungen

angeben. Unter "Value Provider" können Sie die Einstellungen angeben, die für den ausgewählten Wertanbietertyp spezifisch sind.

Siehe "Definieren von Parametern und Value Providers für einen benutzerdefinierten Bericht" auf Seite 481.

Tabelle D-14 Optionen im Dialogfeld "Parameter wird bearbeitet"

Option	Beschreibung
Name	Damit können Sie den Parameternamen angeben.
Parameter erforderlich	Damit können Sie angeben, ob der Parameter im Bericht erforderlich ist.
Beschreibung	Ermöglicht es, die Parameterbeschreibung anzugeben. Diese Beschreibung wird verwendet, um den Parameter in der Dropdown-Liste "Neue Parameter hinzufügen" zu kennzeichnen.
Typ	Ermöglicht es, den Parametertyp auszuwählen.
Anzeige-/Auswertungsreihenfolge	Die Stellen in der Reihenfolge, an der der Parameter auf der Seite "Bericht" angezeigt wird, und die Stelle in der Reihenfolge, an der der Parameter in der Berichtsabfrage ausgewertet wird. In der Dropdown-Liste können Sie den Wert für die Reihenfolge zwischen 1 und 19 festlegen.
Standardwert	Ermöglicht es, den Standardwert für den Parameter anzugeben. Wenn der Benutzer keinen Wert für den Parameter festlegt, wenn er den Bericht erstellt, wird dieser Wert in der Abfrage verwendet.
Wert testen	Ermöglicht es, den Prüfwert für den Parameter anzugeben. Dieser Wert wird verwendet, wenn Sie die Abfrage prüfen.
Value Provider	Ermöglicht es, den Wertanbieter für den Parameter anzugeben. Die Value Provider-Einstellungen geben den UI-Steuerelementtyp an, der für den Benutzer zur Verfügung steht. Für jedes UI Steuerelement können Sie die relevanten Einstellungen festlegen, wie beispielsweise Breite, Bezeichnungstext und QuickInfo des UI-Steuerelements. Die verfügbaren Value Provider-Typen hängen vom Typ des ausgewählten Parameters ab.

Anhang E

Skriptfähige Felder zum Ändern der Import-/Export- und CMDB-Regeln für Ressourcen

Dieser Anhang enthält folgende Themen:

- Skriptfähige Felder zum Ändern der Import-/Exportregel für Ressourcen und CMDB-Regel

Skriptfähige Felder zum Ändern der Import-/Exportregel für Ressourcen und CMDB-Regel

Wenn Sie mit Import-/Exportregel für Ressourcen oder CMDB-Regeln arbeiten, werden Werte für die Spalten des angegebenen Ressourcentyps in der CMDB zugeordnet bzw. festgelegt. Das Verwenden eines Ausdrucks ist eine der Möglichkeiten für das Festlegen von Spaltenwerten. Mit einem Ausdruck können Sie .NET-Skripts schreiben.

Das Erstellen von Ausdrücken wird in den folgenden Themen dokumentiert:

- Siehe "Ausdruckssyntax" auf Seite 574.
- Siehe "Ausdrucksoperatoren" auf Seite 575.
- Siehe "Benutzerdefinierte Werte" auf Seite 575.
- Siehe "Zeichenfolgenoperatoren" auf Seite 575.
- Siehe "Platzhalterzeichen" auf Seite 576.

- Siehe "Aggregationstypen" auf Seite 576.
- Siehe "Ausdrucksfunktionen" auf Seite 576.

Ausdruckssyntax

Verwenden Sie beim Erstellen eines Ausdrucks zum Ändern von Import-/Exportregeln für Ressourcen oder CMDB-Regeln die Eigenschaft "ColumnName" zum Verweisen auf Spalten. Beispiel: Wenn "ColumnName" für eine Spalte "UnitPrice" und eine andere "Quantity" ist, lautet der Ausdruck "UnitPrice * Quantity".

Wenn Sie einen Ausdruck für einen Filter erstellen, schließen Sie Zeichenketten mit einfachen Anführungszeichen ein. Beispiel:

```
'LastName = 'Jones'.'
```

Wenn Sie die folgenden Sonderzeichen in einem Spaltennamen verwenden, müssen Escape-Zeichen vorangestellt werden:

\n (neue Zeile)	\	*	[	"
\t (Tabulator)	/	%	]	#
\r (Wagenrücklauf)	=	&	'	-
~	>	|	+	)
(	<	^		

Enthält ein Spaltenname eins der Zeichen aus der vorhergehenden Tabelle, muss der Name in eckige Klammern gesetzt werden. Beispiel: Wenn Sie den Spaltenamen "Column#" in einem Ausdruck verwenden möchten, müssen Sie Folgendes eingeben:

```
[Column#]". Beispiel: Total * [Column#]
```

Wenn Sie ein Datum eingeben, müssen Sie das Format "Monat/Tag/Jahr" verwenden. Die Formate "Tag/Monat/Jahr" oder "Jahr/Monat/Tag" sind ungültig.

Da eckige Klammern Sonderzeichen sind, müssen Sie einen Schrägstrich ("\") als Escape-Zeichen verwenden, wenn sie Teil eines Spaltenamens sind. Beispiel: Die Spalte "Column[]" sieht dann folgendermaßen aus:

```
"Total * [Column[\]]"
```

Nur die zweite Klammer muss mit einem Escape-Zeichen versehen werden.

Siehe "Skriptfähige Felder zum Ändern der Import-/Exportregel für Ressourcen und CMDB-Regel" auf Seite 573.

Ausdrucksoperatoren

Verkettung wird in Ausdrücke unter Verwendung der Booleschen Operatoren "AND", "OR" und "NOT" unterstützt. Sie können Klammern verwenden, um Klauseln zu gruppieren und Vorrang zu erzwingen. Der Operator "AND" hat Vorrang über anderen Operatoren. Beispiel: (LastName = 'Smith' OR LastName = 'Jones') AND FirstName = 'John'

Beim Erstellen von Vergleichsausdrücken sind folgende Operatoren zulässig:

<	>	<=	>=	<>
=	IN	LIKE		

Beim Erstellen von arithmetischen Vergleichsausdrücken sind folgende Operatoren zulässig:

+ (Addition)	- (Subtraktion)	* (Multiplikation)	/ (Division)	% (Modul)

Siehe "Skriptfähige Felder zum Ändern der Import-/Exportregel für Ressourcen und CMDB-Regel" auf Seite 573.

Benutzerdefinierte Werte

Benutzerdefinierte Werte können in Ausdrücken mit Spaltenwerten verglichen werden. Zeichenkettenwerte sollten in einfachen Anführungszeichen stehen. Datumswerte sollten in Pfundzeichen (#) stehen. Dezimalstellen und wissenschaftliche Formeln sind für numerische Werte zulässig. Beispiele: "FirstName = 'John'"; "Price <= 50.00"; "Birthdate < #1/31/ 82#".

Für die Spalten, die Aufzählungswerte enthalten, legen Sie den Wert als Ganzzahl fest. Beispiel: "EnumColumn = 5"

Siehe "Skriptfähige Felder zum Ändern der Import-/Exportregel für Ressourcen und CMDB-Regel" auf Seite 573.

Zeichenfolgenoperatoren

Verwenden Sie zum Verketten von Zeichenfolgen in einem Ausdruck das Zeichen "+".

Siehe "Skriptfähige Felder zum Ändern der Import-/Exportregel für Ressourcen und CMDB-Regel" auf Seite 573.

Platzhalterzeichen

"*" und "%" können in Ausdrücken als Platzhalter in einem LIKE-Vergleich austauschbar verwendet werden. Wenn die Zeichenfolge in einer LIKE-Klausel ein "*" oder "%" enthält, sollten diese Zeichen in eckige Klammern ([]) gesetzt werden. Enthält die Klausel eine Klammer, sollten die Klammerzeichen in Klammern gesetzt werden. Beispiel: [[] oder []]. Ein Platzhalter ist an Beginn und Ende eines Musters oder nur am Ende eines Musters oder nur am Beginn eines Musters möglich. Beispiele: "ItemName LIKE '*product*'"; "ItemName LIKE '*product'"; "ItemName LIKE 'product*'".

Platzhalter sind innerhalb von Zeichenfolgen nicht zulässig. Beispielsweise ist "te*xt" ungültig.

Siehe "Skriptfähige Felder zum Ändern der Import-/Exportregel für Ressourcen und CMDB-Regel" auf Seite 573.

Aggregationstypen

Sie können folgende Aggregationstypen in Ausdrücken verwenden:

Sum (Summe)	Avg (Durchschnitt)	Min (Minimum)	Max (Maximum)
Count (Anzahl)	StDev (statistische Standardabweichung)	Var (statistische Variation)	

Sie können einen Aggregationsausdruck mit einer der oben genannten Funktionen erstellen. Beispiels: "Sum(Preis) erstellt eine Übersicht von Zahlen in einer Spalte namens "Preis". Da es keine Gruppierungsfunktion gibt, wird in allen Zeilen derselbe Wert in der Spalte angezeigt. Enthält eine Tabelle keine Zeilen, geben Aggregationsfunktionen einen Nullwert aus.

Siehe "Skriptfähige Felder zum Ändern der Import-/Exportregel für Ressourcen und CMDB-Regel" auf Seite 573.

Siehe "Die Funktion "Convert"" auf Seite 577.

Ausdrucksfunktionen

Sie können aus folgenden Ausdrucksfunktionen wählen:

- Convert
  Siehe "Die Funktion "Convert"" auf Seite 577.
- Len
  Siehe "Funktion "Len"" auf Seite 577.
- IsNull

Siehe "Funktion "IsNull"" auf Seite 578.

- IIF
  Siehe "Funktion "IIF"" auf Seite 578.
- Trim
  Siehe "Funktion "Trim"" auf Seite 579.
- Substring
  Siehe "Funktion "Substring"" auf Seite 579.

Siehe "Skriptfähige Felder zum Ändern der Import-/Exportregel für Ressourcen und CMDB-Regel" auf Seite 573.

Die Funktion "Convert"

Konvertiert einen Ausdruck in einen angegebenen .NET Framework-Typ.

Syntax: `Convert(Ausdruck, Typ)`

Tabelle E-1 Argumente der Funktion "Convert"

Argument	Beschreibung
Ausdruck	Der zu konvertierende Ausdruck.
Typ	Der .NET Framework-Typ, in den der Wert konvertiert wird.

Beispiel: `myDataColumn.Expression="Convert(total, 'System.Int32')"`

Alle Konvertierungen sind gültig, mit folgenden Ausnahmen:

- "Boolean" kann nur aus und in Byte, SByte, Int16, Int32, Int64, UInt16, UInt32, UInt64, String und sich selbst umgewandelt werden.
- "Char" kann nur aus und in Int32, UInt32, String und sich selbst umgewandelt werden.
- "DateTime" kann nur aus und in String und sich selbst umgewandelt werden.
- "TimeSpan" kann nur aus und in String und sich selbst umgewandelt werden.

Siehe "Ausdrucksfunktionen" auf Seite 576.

Funktion "Len"

Ruft die Länge einer Zeichenfolge ab.

Syntax: `Len(Ausdruck)`

Tabelle E-2 Argumente der Funktion "Len"

Argument	Beschreibung
Ausdruck	Die zu prüfende Zeichenfolge.

Beispiel: `myDataColumn.Expression="Len(ItemName)"`

Siehe "Ausdrucksfunktionen" auf Seite 576.

Funktion "IsNull"

Prüft einen Ausdruck und gibt entweder den geprüften Ausdruck oder einen Ersatzwert aus.

Syntax: `IsNull(Ausdruck, Ersatzwert)`

Tabelle E-3 Argumente der Funktion "IsNull"

Argument	Beschreibung
Ausdruck	Der zu prüfende Ausdruck.
Ersatzwert	Der Wert, der ausgegeben werden soll, wenn der Ausdruck eine Nullreferenz (nichts) ist.

Beispiel: `myDataColumn.Expression="IsNull(price, -1)"`

Siehe "Ausdrucksfunktionen" auf Seite 576.

Funktion "IIF"

Ruft abhängig von dem Ergebnis eines logischen Ausdrucks einen von zwei Werten ab.

Syntax: `IIF (Ausdruck, wahr, falsch)`

Tabelle E-4 Argumente der Funktion "IIF"

Argument	Beschreibung
Ausdruck	Der auszuwertende Ausdruck.
wahr	Der auszugebende Wert, wenn der Ausdruck wahr ist.
falsch	Der auszugebende Wert, wenn der Ausdruck falsch ist.

Beispiel: `myDataColumn.Expression = "IIF(total>1000, 'expensive', 'dear')`

Siehe "Ausdrucksfunktionen" auf Seite 576.

Funktion "Trim"

Entfernt alle voran- und nachstehenden leeren Zeichen wie \r,\n,\t, ' '

Syntax: `Trim(Ausdruck)`

Tabelle E-5 Argumente der Funktion "Trim"

Argument	Beschreibung
Ausdruck	Definiert den zu bearbeitenden Ausdruck.

Siehe "Ausdrucksfunktionen" auf Seite 576.

Funktion "Substring"

Ruft einen Substring der angegebenen Länge beginnend an einem in der Zeichenfolge angegebenen Punkt ab.

Syntax: `Substring(Ausdruck, Start, Länge)`

Tabelle E-6 Argumente der Funktion "Substring"

Argument	Beschreibung
Ausdruck	Definiert die Quellzeichenfolge für den Substring.
Start	Eine Ganzzahl, die definiert, wo der Substring beginnt.
Länge	Eine Ganzzahl, die die Länge der Substring definiert.

Beispiel: `myDataColumn.Expression = "Substring(Telefon, 7, 8)"`

Sie können die Eigenschaft "Ausdruck" zurücksetzen, indem Sie ihm den Wert "Null" oder eine leere Zeichenfolge zuweisen. Ist ein Standardwert in der Spalte "Ausdruck" festgelegt, werden dieser allen vorher gefüllten Zeilen zugewiesen, nachdem die Eigenschaft "Ausdruck" zurückgesetzt wurde.

Siehe "Ausdrucksfunktionen" auf Seite 576.

Anhang F

Symantec™ Management-Plattform 7.5 - Rechtliche Hinweise zu Drittanbietern

Dieser Anhang enthält folgende Themen:

- Rechtliche Hinweise zu Drittanbietern
- 7-Zip
- Apache HTTP Server
- Apache Xerces C++
- Boost
- Bouncy Castle
- Curl
- glibc
- Libatomics_Ops
- LibXML2
- Makeself
- Microsoft Anti-Cross Site Scripting Library
- OpenPegasus

- OpenSSL 0.9.8u
- OpenSSL 0.9.8y
- OpenSSL 1.0.1e
- plists-cs
- SQLite
- Windows Template Library 'WTL' v8.0
- Zlib

Rechtliche Hinweise zu Drittanbietern

Dieses Symantec-Produkt kann Drittanbietersoftware enthalten, für die Symantec die Rechte der Drittanbieter (“Nicht-Symantec-Programme”) anerkennt. Einige Nicht-Symantec-Programme sind als “open source” oder als freie Softwarelizenzen verfügbar. Die Lizenzvereinbarung dieser Software hat keinen Einfluss auf Ihre Rechte oder Pflichten, die im Rahmen solcher Open Source- oder freien Softwarelizenzen gelten. Dieser Anhang enthält Hinweise zu den Eigentumsrechten sowie gegebenenfalls zu den Lizenzen der Drittanbietersoftware.

7-Zip

7-Zip v9.20 [2010-11-18] for Windows

Copyright (c) 1999-2010 Igor Pavlov

All copyrights to original unRAR code are owned by Alexander Roshal

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder” in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Apache HTTP Server

Apache HTTP Server v2.2.22

Portions of this program contain components from the Apache Software Foundation. These components are made available under the Apache License 2.0, a copy of which is provided herein.

Apache License, Version 2.0

January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation

against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.

You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- You must give any other recipients of the Work or Derivative Works a copy of this License; and
- You must cause any modified files to carry prominent notices stating that You changed the files; and
- You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions.

Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks.

This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty.

Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE, NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Apache Xerces C++

Apache Xerces C++ v3.0

Copyright © 2012 The Apache Software Foundation, Licensed under the Apache License, Version 2.0.

Apache and the Apache feather logo are trademarks of The Apache Software Foundation.

Apache License, Version 2.0

January 2004

http://www.apache.org/licenses/

TERMS AND CONDITIONS FOR USE, REPRODUCTION, AND DISTRIBUTION

1. Definitions.

"License" shall mean the terms and conditions for use, reproduction, and distribution as defined by Sections 1 through 9 of this document.

"Licensor" shall mean the copyright owner or entity authorized by the copyright owner that is granting the License.

"Legal Entity" shall mean the union of the acting entity and all other entities that control, are controlled by, or are under common control with that entity. For the purposes of this definition, "control" means (i) the power, direct or indirect, to cause the direction or management of such entity, whether by contract or otherwise, or (ii) ownership of fifty percent (50%) or more of the outstanding shares, or (iii) beneficial ownership of such entity.

"You" (or "Your") shall mean an individual or Legal Entity exercising permissions granted by this License.

"Source" form shall mean the preferred form for making modifications, including but not limited to software source code, documentation source, and configuration files.

"Object" form shall mean any form resulting from mechanical transformation or translation of a Source form, including but not limited to compiled object code, generated documentation, and conversions to other media types.

"Work" shall mean the work of authorship, whether in Source or Object form, made available under the License, as indicated by a copyright notice that is included in or attached to the work (an example is provided in the Appendix below).

"Derivative Works" shall mean any work, whether in Source or Object form, that is based on (or derived from) the Work and for which the editorial revisions, annotations, elaborations, or other modifications represent, as a whole, an original work of authorship. For the purposes of this License, Derivative Works shall not include works that remain separable from, or merely link (or bind by name) to the interfaces of, the Work and Derivative Works thereof.

"Contribution" shall mean any work of authorship, including the original version of the Work and any modifications or additions to that Work or Derivative Works thereof, that is intentionally submitted to Licensor for inclusion in the Work by the copyright owner or by an individual or Legal Entity authorized to submit on behalf of the copyright owner. For the purposes of this definition, "submitted" means any form of electronic, verbal, or written communication sent to the Licensor or its representatives, including but not limited to communication on electronic mailing lists, source code control systems, and issue tracking systems that are managed by, or on behalf of, the Licensor for the purpose of discussing and improving the Work, but excluding communication that is conspicuously marked or otherwise designated in writing by the copyright owner as "Not a Contribution."

"Contributor" shall mean Licensor and any individual or Legal Entity on behalf of whom a Contribution has been received by Licensor and subsequently incorporated within the Work.

2. Grant of Copyright License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable copyright license to reproduce, prepare Derivative Works of, publicly display, publicly perform, sublicense, and distribute the Work and such Derivative Works in Source or Object form.

3. Grant of Patent License.

Subject to the terms and conditions of this License, each Contributor hereby grants to You a perpetual, worldwide, non-exclusive, no-charge, royalty-free, irrevocable (except as stated in this section) patent license to make, have made, use, offer to sell, sell, import, and otherwise transfer the Work, where such license applies only to those patent claims licensable by such Contributor that are necessarily infringed by their Contribution(s) alone or by combination of their Contribution(s) with the Work to which such Contribution(s) was submitted. If You institute patent litigation against any entity (including a cross-claim or counterclaim in a lawsuit) alleging that the Work or a Contribution incorporated within the Work constitutes direct or contributory patent infringement, then any patent licenses granted to You under this License for that Work shall terminate as of the date such litigation is filed.

4. Redistribution.

You may reproduce and distribute copies of the Work or Derivative Works thereof in any medium, with or without modifications, and in Source or Object form, provided that You meet the following conditions:

- You must give any other recipients of the Work or Derivative Works a copy of this License; and

- You must cause any modified files to carry prominent notices stating that You changed the files; and
- You must retain, in the Source form of any Derivative Works that You distribute, all copyright, patent, trademark, and attribution notices from the Source form of the Work, excluding those notices that do not pertain to any part of the Derivative Works; and
- If the Work includes a "NOTICE" text file as part of its distribution, then any Derivative Works that You distribute must include a readable copy of the attribution notices contained within such NOTICE file, excluding those notices that do not pertain to any part of the Derivative Works, in at least one of the following places: within a NOTICE text file distributed as part of the Derivative Works; within the Source form or documentation, if provided along with the Derivative Works; or, within a display generated by the Derivative Works, if and wherever such third-party notices normally appear. The contents of the NOTICE file are for informational purposes only and do not modify the License. You may add Your own attribution notices within Derivative Works that You distribute, alongside or as an addendum to the NOTICE text from the Work, provided that such additional attribution notices cannot be construed as modifying the License.

You may add Your own copyright statement to Your modifications and may provide additional or different license terms and conditions for use, reproduction, or distribution of Your modifications, or for any such Derivative Works as a whole, provided Your use, reproduction, and distribution of the Work otherwise complies with the conditions stated in this License.

5. Submission of Contributions.

Unless You explicitly state otherwise, any Contribution intentionally submitted for inclusion in the Work by You to the Licensor shall be under the terms and conditions of this License, without any additional terms or conditions. Notwithstanding the above, nothing herein shall supersede or modify the terms of any separate license agreement you may have executed with Licensor regarding such Contributions.

6. Trademarks.

This License does not grant permission to use the trade names, trademarks, service marks, or product names of the Licensor, except as required for reasonable and customary use in describing the origin of the Work and reproducing the content of the NOTICE file.

7. Disclaimer of Warranty.

Unless required by applicable law or agreed to in writing, Licensor provides the Work (and each Contributor provides its Contributions) on an "AS IS" BASIS, WITHOUT WARRANTIES OR CONDITIONS OF ANY KIND, either express or implied, including, without limitation, any warranties or conditions of TITLE,

NON-INFRINGEMENT, MERCHANTABILITY, or FITNESS FOR A PARTICULAR PURPOSE. You are solely responsible for determining the appropriateness of using or redistributing the Work and assume any risks associated with Your exercise of permissions under this License.

8. Limitation of Liability.

In no event and under no legal theory, whether in tort (including negligence), contract, or otherwise, unless required by applicable law (such as deliberate and grossly negligent acts) or agreed to in writing, shall any Contributor be liable to You for damages, including any direct, indirect, special, incidental, or consequential damages of any character arising as a result of this License or out of the use or inability to use the Work (including but not limited to damages for loss of goodwill, work stoppage, computer failure or malfunction, or any and all other commercial damages or losses), even if such Contributor has been advised of the possibility of such damages.

9. Accepting Warranty or Additional Liability.

While redistributing the Work or Derivative Works thereof, You may choose to offer, and charge a fee for, acceptance of support, warranty, indemnity, or other liability obligations and/or rights consistent with this License. However, in accepting such obligations, You may act only on Your own behalf and on Your sole responsibility, not on behalf of any other Contributor, and only if You agree to indemnify, defend, and hold each Contributor harmless for any liability incurred by, or claims asserted against, such Contributor by reason of your accepting any such warranty or additional liability.

END OF TERMS AND CONDITIONS

Boost

Boost v1.42.0

Copyright Joe Coder 2004 - 2006.

Boost Software License - Version 1.0 - August 17th, 2003

Permission is hereby granted, free of charge, to any person or organization obtaining a copy of the software and accompanying documentation covered by this license (the "Software") to use, reproduce, display, distribute, execute, and transmit the Software, and to prepare derivative works of the Software, and to permit third-parties to whom the Software is furnished to do so, all subject to the following:

The copyright notices in the Software and this entire statement, including the above license grant, this restriction and the following disclaimer, must be included in all copies of the Software, in whole or in part, and all derivative works of the Software,

unless such copies or derivative works are solely in the form of machine-executable object code generated by a source language processor.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE, TITLE AND NON-INFRINGEMENT. IN NO EVENT SHALL THE COPYRIGHT HOLDERS OR ANYONE DISTRIBUTING THE SOFTWARE BE LIABLE FOR ANY DAMAGES OR OTHER LIABILITY, WHETHER IN CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Bouncy Castle

Bouncy Castle v1.5

The Legion Of The Bouncy Castle

Copyright (c) 2000 - 2010 The Legion Of The Bouncy Castle (http://www.bouncycastle.org)

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder" in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Curl

Curl v7.24.0

Copyright (c) 1996 - 2011, Daniel Stenberg, <daniel@haxx.se>.All rights reserved

COPYRIGHT AND PERMISSION NOTICE

Copyright (c) 1996 - 2011, Daniel Stenberg, <daniel@haxx.se>.

All rights reserved.

Permission to use, copy, modify, and distribute this software for any purpose with or without fee is hereby granted, provided that the above copyright notice and this permission notice appear in all copies.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT OF THIRD PARTY RIGHTS. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Except as contained in this notice, the name of a copyright holder shall not be used in advertising or otherwise to promote the sale, use or other dealings in this Software without prior written authorization of the copyright holder.

glibc

glibc i686 rpm v2.12-1.7

Free Software Foundation, a wide variety of years

Copyright (C) 1991 Regents of the University of California.

Portions Copyright (C) 1993 by Digital Equipment Corporation.

Copyright (C) 1984, Sun Microsystems, Inc.

Copyright (C) 1991,1990,1989 Carnegie Mellon University

Copyright (c) 2000, Intel Corporation copyright (C) by Craig Metz, no year specified

The code may be accessed at: http://rhn.redhat.com

GNU Lesser General Public License

Version 2.1, February 1999

Copyright (C) 1991, 1999 Free Software Foundation, Inc. 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

[This is the first released version of the Lesser GPL. It also counts as the successor of the GNU Library Public License, version 2, hence the version number 2.1.]

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users.

This license, the Lesser General Public License, applies to some specially designated software packages--typically libraries--of the Free Software Foundation and other authors who decide to use it. You can use it too, but we suggest you first think carefully about whether this license or the ordinary General Public License is the better strategy to use in any particular case, based on the explanations below.

When we speak of free software, we are referring to freedom of use, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish); that you receive source code or can get it if you want it; that you can change the software and use pieces of it in new free programs; and that you are informed that you can do these things.

To protect your rights, we need to make restrictions that forbid distributors to deny you these rights or to ask you to surrender these rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you. You must make sure that they, too, receive or can get the source code. If you link other code with the library, you must provide complete object files to the recipients, so that they can relink them with the library after making changes to the library and recompiling it. And you must show them these terms so they know their rights.

We protect your rights with a two-step method: (1) we copyright the library, and (2) we offer you this license, which gives you legal permission to copy, distribute and/or modify the library.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

To protect each distributor, we want to make it very clear that there is no warranty for the free library. Also, if the library is modified by someone else and passed on, the recipients should know that what they have is not the original version, so that the original author's reputation will not be affected by problems that might be introduced by others.

Most GNU software, including some libraries, is covered by the ordinary GNU General Public License. This license, the GNU Lesser General Public License, applies to certain designated libraries, and is quite different from the ordinary General Public License. We use this license for certain libraries in order to permit linking those libraries into non-free programs.

When a program is linked with a library, whether statically or using a shared library, the combination of the two is legally speaking a combined work, a derivative of the original library. The ordinary General Public License therefore permits such linking only if the entire combination fits its criteria of freedom. The Lesser General Public License permits more lax criteria for linking other code with the library.

We call this license the "Lesser" General Public License because it does Less to protect the user's freedom than the ordinary General Public License. It also provides other free software developers Less of an advantage over competing non-free programs. These disadvantages are the reason we use the ordinary General Public License for many libraries. However, the Lesser license provides advantages in certain special circumstances.

For example, on rare occasions, there may be a special need to encourage the widest possible use of a certain library, so that it becomes a de-facto standard. To achieve this, non-free programs must be allowed to use the library. A more frequent case is that a free library does the same job as widely used non-free libraries. In this case, there is little to gain by limiting the free library to free software only, so we use the Lesser General Public License.

In other cases, permission to use a particular library in non-free programs enables a greater number of people to use a large body of free software. For example, permission to use the GNU C Library in non-free programs enables many more people to use the whole GNU operating system, as well as its variant, the GNU/Linux operating system.

Although the Lesser General Public License is Less protective of the users' freedom, it does ensure that the user of a program that is linked with the Library has the freedom and the wherewithal to run that program using a modified version of the Library.

The precise terms and conditions for copying, distribution and modification follow. Pay close attention to the difference between a "work based on the library" and a "work that uses the library". The former contains code derived from the library, whereas the latter must be combined with the library in order to run.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License Agreement applies to any software library or other program which contains a notice placed by the copyright holder or other authorized party saying it may be distributed under the terms of this Lesser General Public License (also called "this License"). Each licensee is addressed as "you".

A "library" means a collection of software functions and/or data prepared so as to be conveniently linked with application programs (which use some of those functions and data) to form executables.

The "Library", below, refers to any such software library or work which has been distributed under these terms. A "work based on the Library" means either the Library or any derivative work under copyright law: that is to say, a work containing the Library or a portion of it, either verbatim or with modifications and/or translated straightforwardly into another language. (Hereinafter, translation is included without limitation in the term "modification".)

"Source code" for a work means the preferred form of the work for making modifications to it. For a library, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the library.

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running a program using the Library is not restricted, and output from such a program is covered only if its contents constitute a work based on the Library (independent of the use of the Library in a tool for writing it). Whether that is true depends on what the Library does and what the program that uses the Library does.

1. You may copy and distribute verbatim copies of the Library's complete source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and distribute a copy of this License along with the Library.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Library or any portion of it, thus forming a work based on the Library, and copy and distribute such modifications or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) The modified work must itself be a software library.

b) You must cause the files modified to carry prominent notices stating that you changed the files and the date of any change.

c) You must cause the whole of the work to be licensed at no charge to all third parties under the terms of this License.

d) If a facility in the modified Library refers to a function or a table of data to be supplied by an application program that uses the facility, other than as an argument passed when the facility is invoked, then you must make a good faith effort to ensure that, in the event an application does not supply such function or table, the facility still operates, and performs whatever part of its purpose remains meaningful.

(For example, a function in a library to compute square roots has a purpose that is entirely well-defined independent of the application. Therefore, Subsection 2d requires that any application-supplied function or table used by this function must be optional: if the application does not supply it, the square root function must still compute square roots.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Library, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Library, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Library.

In addition, mere aggregation of another work not based on the Library with the Library (or with a work based on the Library) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may opt to apply the terms of the ordinary GNU General Public License instead of this License to a given copy of the Library. To do this, you must alter all the notices that refer to this License, so that they refer to the ordinary GNU General Public License, version 2, instead of to this License. (If a newer version than version 2 of the ordinary GNU General Public License has appeared, then you can specify that version instead if you wish.) Do not make any other change in these notices.

Once this change is made in a given copy, it is irreversible for that copy, so the ordinary GNU General Public License applies to all subsequent copies and derivative works made from that copy.

This option is useful when you wish to copy part of the code of the Library into a program that is not a library.

4. You may copy and distribute the Library (or a portion or derivative of it, under Section 2) in object code or executable form under the terms of Sections 1 and 2

above provided that you accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange.

If distribution of object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place satisfies the requirement to distribute the source code, even though third parties are not compelled to copy the source along with the object code.

5. A program that contains no derivative of any portion of the Library, but is designed to work with the Library by being compiled or linked with it, is called a "work that uses the Library". Such a work, in isolation, is not a derivative work of the Library, and therefore falls outside the scope of this License.

However, linking a "work that uses the Library" with the Library creates an executable that is a derivative of the Library (because it contains portions of the Library), rather than a "work that uses the library". The executable is therefore covered by this License. Section 6 states terms for distribution of such executables.

When a "work that uses the Library" uses material from a header file that is part of the Library, the object code for the work may be a derivative work of the Library even though the source code is not. Whether this is true is especially significant if the work can be linked without the Library, or if the work is itself a library. The threshold for this to be true is not precisely defined by law.

If such an object file uses only numerical parameters, data structure layouts and accessors, and small macros and small inline functions (ten lines or less in length), then the use of the object file is unrestricted, regardless of whether it is legally a derivative work. (Executables containing this object code plus portions of the Library will still fall under Section 6.)

Otherwise, if the work is a derivative of the Library, you may distribute the object code for the work under the terms of Section 6. Any executables containing that work also fall under Section 6, whether or not they are linked directly with the Library itself.

6. As an exception to the Sections above, you may also combine or link a "work that uses the Library" with the Library to produce a work containing portions of the Library, and distribute that work under terms of your choice, provided that the terms permit modification of the work for the customer's own use and reverse engineering for debugging such modifications.

You must give prominent notice with each copy of the work that the Library is used in it and that the Library and its use are covered by this License. You must supply a copy of this License. If the work during execution displays copyright notices, you must include the copyright notice for the Library among them, as well as a reference directing the user to the copy of this License. Also, you must do one of these things:

a) Accompany the work with the complete corresponding machine-readable source code for the Library including whatever changes were used in the work (which must be distributed under Sections 1 and 2 above); and, if the work is an executable linked with the Library, with the complete machine-readable "work that uses the Library", as object code and/or source code, so that the user can modify the Library and then relink to produce a modified executable containing the modified Library. (It is understood that the user who changes the contents of definitions files in the Library will not necessarily be able to recompile the application to use the modified definitions.)

b) Use a suitable shared library mechanism for linking with the Library. A suitable mechanism is one that (1) uses at run time a copy of the library already present on the user's computer system, rather than copying library functions into the executable, and (2) will operate properly with a modified version of the library, if the user installs one, as long as the modified version is interface-compatible with the version that the work was made with.

c) Accompany the work with a written offer, valid for at least three years, to give the same user the materials specified in Subsection 6a, above, for a charge no more than the cost of performing this distribution

d) If distribution of the work is made by offering access to copy from a designated place, offer equivalent access to copy the above specified materials from the same place.

e) Verify that the user has already received a copy of these materials or that you have already sent this user a copy.

For an executable, the required form of the "work that uses the Library" must include any data and utility programs needed for reproducing the executable from it. However, as a special exception, the materials to be distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

It may happen that this requirement contradicts the license restrictions of other proprietary libraries that do not normally accompany the operating system. Such a contradiction means you cannot use both them and the Library together in an executable that you distribute.

7. You may place library facilities that are a work based on the Library side-by-side in a single library together with other library facilities not covered by this License, and distribute such a combined library, provided that the separate distribution of the work based on the Library and of the other library facilities is otherwise permitted, and provided that you do these two things:

a) Accompany the combined library with a copy of the same work based on the Library, uncombined with any other library facilities. This must be distributed under the terms of the Sections above.

b) Give prominent notice with the combined library of the fact that part of it is a work based on the Library, and explaining where to find the accompanying uncombined form of the same work.

8. You may not copy, modify, sublicense, link with, or distribute the Library except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense, link with, or distribute the Library is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

9. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Library or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Library (or any work based on the Library), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Library or works based on it.

10. Each time you redistribute the Library (or any work based on the Library), the recipient automatically receives a license from the original licensor to copy, distribute, link with or modify the Library subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties with this License.

11. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Library at all. For example, if a patent license would not permit royalty-free redistribution of the Library by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Library.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply, and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system which

is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

12. If the distribution and/or use of the Library is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Library under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

13. The Free Software Foundation may publish revised and/or new versions of the Lesser General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Library specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Library does not specify a license version number, you may choose any version ever published by the Free Software Foundation.

14. If you wish to incorporate parts of the Library into other free programs whose distribution conditions are incompatible with these, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

15. BECAUSE THE LIBRARY IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE LIBRARY, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE LIBRARY "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE LIBRARY IS WITH YOU. SHOULD THE

LIBRARY PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

16. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE LIBRARY AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE LIBRARY (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE LIBRARY TO OPERATE WITH ANY OTHER SOFTWARE), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Libraries

If you develop a new library, and you want it to be of the greatest possible use to the public, we recommend making it free software that everyone can redistribute and change. You can do so by permitting redistribution under these terms (or, alternatively, under the terms of the ordinary General Public License).

To apply these terms, attach the following notices to the library. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

<one line to give the library's name and an idea of what it does.> Copyright (C) <year> <name of author>

This library is free software; you can redistribute it and/or modify it under the terms of the GNU Lesser General Public License as published by the Free Software Foundation; either version 2.1 of the License, or (at your option) any later version.

This library is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU Lesser General Public License for more details.

You should have received a copy of the GNU Lesser General Public License along with this library; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the library, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the library `Frob' (a library for tweaking knobs) written by James Random Hacker.

signature of Ty Coon, 1 April 1990 Ty Coon, President of Vice

Libatomics_Ops

Hewlett-Packard Development Company, L.P., Xerox Corporation, Silicon Graphics & Hewlett-Packard Company.

Copyright (c) 2003-2004 Hewlett-Packard Development Company, L.P.

Copyright (c) 1991-1994 by Xerox Corporation. All rights reserved.

Copyright (c) 1996-1999 by Silicon Graphics. All rights reserved.

Copyright (c) 1999-2003 by Hewlett-Packard Company. All rights reserved.

Our intent is to make it easy to use libatomic_ops, in both free and proprietary software. Hence most code that we expect to be linked into a client application is covered by an MIT-style license.

A few library routines are covered by the GNU General Public License. These are put into a separate library, libatomic_ops_gpl.a .

The low-level part of the library is mostly covered by the following license:

Copyright (c) ...

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

A few files in the sysdeps directory were inherited in part from the Boehm-Demers-Weiser conservative garbage collector, and are covered by its license, which is similar in spirit:

Copyright (c) ...

THIS MATERIAL IS PROVIDED AS IS, WITH ABSOLUTELY NO WARRANTY EXPRESSED OR IMPLIED. ANY USE IS AT YOUR OWN RISK.

Permission is hereby granted to use or copy this program for any purpose, provided the above notices are retained on all copies. Permission to modify the code and to distribute modified code is granted, provided the above notices are retained, and a notice that the code was modified is included with the above copyright notice.

A few files are covered by the GNU General Public License. (See file "COPYING".) This applies only to test code, sample applications, and the libatomic_ops_gpl portion of the library. Thus libatomic_ops_gpl should generally not be linked into proprietary code. (This distinction was motivated by patent considerations.)

It is possible that the license of the GPL pieces may be changed for future versions to make them more consistent with the rest of the package. If you submit patches, and have strong preferences about licensing, please express them.

LibXML2

Copyright (C) 1998-2003 Daniel Veillard. All Rights Reserved.

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder” in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY,

WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

Makeself

Makeself v2.1.5

(C) 1998-2008 by Stéphane Peter <megastep@megastep.org>

The source code for this component may be obtained from Symantec Corporation upon request.

The GNU General Public License (GPL)

Version 2, June 1991

Copyright (C) 1989, 1991 Free Software Foundation, Inc.

59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Everyone is permitted to copy and distribute verbatim copies of this license document, but changing it is not allowed.

Preamble

The licenses for most software are designed to take away your freedom to share and change it. By contrast, the GNU General Public License is intended to guarantee your freedom to share and change free software--to make sure the software is free for all its users. This General Public License applies to most of the Free Software Foundation's software and to any other program whose authors commit to using it. (Some other Free Software Foundation software is covered by the GNU Library General Public License instead.) You can apply it to your programs, too.

When we speak of free software, we are referring to freedom, not price. Our General Public Licenses are designed to make sure that you have the freedom to distribute copies of free software (and charge for this service if you wish), that you receive source code or can get it if you want it, that you can change the software or use pieces of it in new free programs; and that you know you can do these things.

To protect your rights, we need to make restrictions that forbid anyone to deny you these rights or to ask you to surrender the rights. These restrictions translate to certain responsibilities for you if you distribute copies of the software, or if you modify it.

For example, if you distribute copies of such a program, whether gratis or for a fee, you must give the recipients all the rights that you have. You must make sure that they, too, receive or can get the source code. And you must show them these terms so they know their rights.

We protect your rights with two steps: (1) copyright the software, and (2) offer you this license which gives you legal permission to copy, distribute and/or modify the software.

Also, for each author's protection and ours, we want to make certain that everyone understands that there is no warranty for this free software. If the software is modified by someone else and passed on, we want its recipients to know that what they have is not the original, so that any problems introduced by others will not reflect on the original authors' reputations.

Finally, any free program is threatened constantly by software patents. We wish to avoid the danger that redistributors of a free program will individually obtain patent licenses, in effect making the program proprietary. To prevent this, we have made it clear that any patent must be licensed for everyone's free use or not licensed at all.

The precise terms and conditions for copying, distribution and modification follow.

TERMS AND CONDITIONS FOR COPYING, DISTRIBUTION AND MODIFICATION

0. This License applies to any program or other work which contains a notice placed by the copyright holder saying it may be distributed under the terms of this General Public License. The "Program", below, refers to any such program or work, and a "work based on the Program" means either the Program or any derivative work under copyright law: that is to say, a work containing the Program or a portion of it, either verbatim or with modifications and/or translated into another language. (Hereinafter, translation is included without limitation in the term "modification".) Each licensee is addressed as "you".

Activities other than copying, distribution and modification are not covered by this License; they are outside its scope. The act of running the Program is not restricted, and the output from the Program is covered only if its contents constitute a work based on the Program (independent of having been made by running the Program). Whether that is true depends on what the Program does.

1. You may copy and distribute verbatim copies of the Program's source code as you receive it, in any medium, provided that you conspicuously and appropriately publish on each copy an appropriate copyright notice and disclaimer of warranty; keep intact all the notices that refer to this License and to the absence of any warranty; and give any other recipients of the Program a copy of this License along with the Program.

You may charge a fee for the physical act of transferring a copy, and you may at your option offer warranty protection in exchange for a fee.

2. You may modify your copy or copies of the Program or any portion of it, thus forming a work based on the Program, and copy and distribute such modifications

or work under the terms of Section 1 above, provided that you also meet all of these conditions:

a) You must cause the modified files to carry prominent notices stating that you changed the files and the date of any change.

b) You must cause any work that you distribute or publish, that in whole or in part contains or is derived from the Program or any part thereof, to be licensed as a whole at no charge to all third parties under the terms of this License.

c) If the modified program normally reads commands interactively when run, you must cause it, when started running for such interactive use in the most ordinary way, to print or display an announcement including an appropriate copyright notice and a notice that there is no warranty (or else, saying that you provide a warranty) and that users may redistribute the program under these conditions, and telling the user how to view a copy of this License. (Exception: if the Program itself is interactive but does not normally print such an announcement, your work based on the Program is not required to print an announcement.)

These requirements apply to the modified work as a whole. If identifiable sections of that work are not derived from the Program, and can be reasonably considered independent and separate works in themselves, then this License, and its terms, do not apply to those sections when you distribute them as separate works. But when you distribute the same sections as part of a whole which is a work based on the Program, the distribution of the whole must be on the terms of this License, whose permissions for other licensees extend to the entire whole, and thus to each and every part regardless of who wrote it.

Thus, it is not the intent of this section to claim rights or contest your rights to work written entirely by you; rather, the intent is to exercise the right to control the distribution of derivative or collective works based on the Program.

In addition, mere aggregation of another work not based on the Program with the Program (or with a work based on the Program) on a volume of a storage or distribution medium does not bring the other work under the scope of this License.

3. You may copy and distribute the Program (or a work based on it, under Section 2) in object code or executable form under the terms of Sections 1 and 2 above provided that you also do one of the following:

a) Accompany it with the complete corresponding machine-readable source code, which must be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

b) Accompany it with a written offer, valid for at least three years, to give any third party, for a charge no more than your cost of physically performing source distribution, a complete machine-readable copy of the corresponding source code,

to be distributed under the terms of Sections 1 and 2 above on a medium customarily used for software interchange; or,

c) Accompany it with the information you received as to the offer to distribute corresponding source code. (This alternative is allowed only for noncommercial distribution and only if you received the program in object code or executable form with such an offer, in accord with Subsection b above.)

The source code for a work means the preferred form of the work for making modifications to it. For an executable work, complete source code means all the source code for all modules it contains, plus any associated interface definition files, plus the scripts used to control compilation and installation of the executable. However, as a special exception, the source code distributed need not include anything that is normally distributed (in either source or binary form) with the major components (compiler, kernel, and so on) of the operating system on which the executable runs, unless that component itself accompanies the executable.

If distribution of executable or object code is made by offering access to copy from a designated place, then offering equivalent access to copy the source code from the same place counts as distribution of the source code, even though third parties are not compelled to copy the source along with the object code.

4. You may not copy, modify, sublicense, or distribute the Program except as expressly provided under this License. Any attempt otherwise to copy, modify, sublicense or distribute the Program is void, and will automatically terminate your rights under this License. However, parties who have received copies, or rights, from you under this License will not have their licenses terminated so long as such parties remain in full compliance.

5. You are not required to accept this License, since you have not signed it. However, nothing else grants you permission to modify or distribute the Program or its derivative works. These actions are prohibited by law if you do not accept this License. Therefore, by modifying or distributing the Program (or any work based on the Program), you indicate your acceptance of this License to do so, and all its terms and conditions for copying, distributing or modifying the Program or works based on it.

6. Each time you redistribute the Program (or any work based on the Program), the recipient automatically receives a license from the original licensor to copy, distribute or modify the Program subject to these terms and conditions. You may not impose any further restrictions on the recipients' exercise of the rights granted herein. You are not responsible for enforcing compliance by third parties to this License.

7. If, as a consequence of a court judgment or allegation of patent infringement or for any other reason (not limited to patent issues), conditions are imposed on you (whether by court order, agreement or otherwise) that contradict the conditions of this License, they do not excuse you from the conditions of this License. If you

cannot distribute so as to satisfy simultaneously your obligations under this License and any other pertinent obligations, then as a consequence you may not distribute the Program at all. For example, if a patent license would not permit royalty-free redistribution of the Program by all those who receive copies directly or indirectly through you, then the only way you could satisfy both it and this License would be to refrain entirely from distribution of the Program.

If any portion of this section is held invalid or unenforceable under any particular circumstance, the balance of the section is intended to apply and the section as a whole is intended to apply in other circumstances.

It is not the purpose of this section to induce you to infringe any patents or other property right claims or to contest validity of any such claims; this section has the sole purpose of protecting the integrity of the free software distribution system, which is implemented by public license practices. Many people have made generous contributions to the wide range of software distributed through that system in reliance on consistent application of that system; it is up to the author/donor to decide if he or she is willing to distribute software through any other system and a licensee cannot impose that choice.

This section is intended to make thoroughly clear what is believed to be a consequence of the rest of this License.

8. If the distribution and/or use of the Program is restricted in certain countries either by patents or by copyrighted interfaces, the original copyright holder who places the Program under this License may add an explicit geographical distribution limitation excluding those countries, so that distribution is permitted only in or among countries not thus excluded. In such case, this License incorporates the limitation as if written in the body of this License.

9. The Free Software Foundation may publish revised and/or new versions of the General Public License from time to time. Such new versions will be similar in spirit to the present version, but may differ in detail to address new problems or concerns.

Each version is given a distinguishing version number. If the Program specifies a version number of this License which applies to it and "any later version", you have the option of following the terms and conditions either of that version or of any later version published by the Free Software Foundation. If the Program does not specify a version number of this License, you may choose any version ever published by the Free Software Foundation.

10. If you wish to incorporate parts of the Program into other free programs whose distribution conditions are different, write to the author to ask for permission. For software which is copyrighted by the Free Software Foundation, write to the Free Software Foundation; we sometimes make exceptions for this. Our decision will be guided by the two goals of preserving the free status of all derivatives of our free software and of promoting the sharing and reuse of software generally.

NO WARRANTY

11. BECAUSE THE PROGRAM IS LICENSED FREE OF CHARGE, THERE IS NO WARRANTY FOR THE PROGRAM, TO THE EXTENT PERMITTED BY APPLICABLE LAW. EXCEPT WHEN OTHERWISE STATED IN WRITING THE COPYRIGHT HOLDERS AND/OR OTHER PARTIES PROVIDE THE PROGRAM "AS IS" WITHOUT WARRANTY OF ANY KIND, EITHER EXPRESSED OR IMPLIED, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE. THE ENTIRE RISK AS TO THE QUALITY AND PERFORMANCE OF THE PROGRAM IS WITH YOU. SHOULD THE PROGRAM PROVE DEFECTIVE, YOU ASSUME THE COST OF ALL NECESSARY SERVICING, REPAIR OR CORRECTION.

12. IN NO EVENT UNLESS REQUIRED BY APPLICABLE LAW OR AGREED TO IN WRITING WILL ANY COPYRIGHT HOLDER, OR ANY OTHER PARTY WHO MAY MODIFY AND/OR REDISTRIBUTE THE PROGRAM AS PERMITTED ABOVE, BE LIABLE TO YOU FOR DAMAGES, INCLUDING ANY GENERAL, SPECIAL, INCIDENTAL OR CONSEQUENTIAL DAMAGES ARISING OUT OF THE USE OR INABILITY TO USE THE PROGRAM (INCLUDING BUT NOT LIMITED TO LOSS OF DATA OR DATA BEING RENDERED INACCURATE OR LOSSES SUSTAINED BY YOU OR THIRD PARTIES OR A FAILURE OF THE PROGRAM TO OPERATE WITH ANY OTHER PROGRAMS), EVEN IF SUCH HOLDER OR OTHER PARTY HAS BEEN ADVISED OF THE POSSIBILITY OF SUCH DAMAGES.

END OF TERMS AND CONDITIONS

How to Apply These Terms to Your New Programs

If you develop a new program, and you want it to be of the greatest possible use to the public, the best way to achieve this is to make it free software which everyone can redistribute and change under these terms.

To do so, attach the following notices to the program. It is safest to attach them to the start of each source file to most effectively convey the exclusion of warranty; and each file should have at least the "copyright" line and a pointer to where the full notice is found.

One line to give the program's name and a brief idea of what it does. Copyright (C) <year> <name of author>

This program is free software; you can redistribute it and/or modify it under the terms of the GNU General Public License as published by the Free Software Foundation; either version 2 of the License, or (at your option) any later version.

This program is distributed in the hope that it will be useful, but WITHOUT ANY WARRANTY; without even the implied warranty of MERCHANTABILITY or FITNESS FOR A PARTICULAR PURPOSE. See the GNU General Public License for more details.

You should have received a copy of the GNU General Public License along with this program; if not, write to the Free Software Foundation, Inc., 59 Temple Place, Suite 330, Boston, MA 02111-1307 USA

Also add information on how to contact you by electronic and paper mail.

If the program is interactive, make it output a short notice like this when it starts in an interactive mode:

Gnomovision version 69, Copyright (C) year name of author Gnomovision comes with ABSOLUTELY NO WARRANTY; for details type `show w'. This is free software, and you are welcome to redistribute it under certain conditions; type `show c' for details.

The hypothetical commands `show w' and `show c' should show the appropriate parts of the General Public License. Of course, the commands you use may be called something other than `show w' and `show c'; they could even be mouse-clicks or menu items--whatever suits your program.

You should also get your employer (if you work as a programmer) or your school, if any, to sign a "copyright disclaimer" for the program, if necessary. Here is a sample; alter the names:

Yoyodyne, Inc., hereby disclaims all copyright interest in the program `Gnomovision' (which makes passes at compilers) written by James Hacker.

signature of Ty Coon, 1 April 1989

Ty Coon, President of Vice

This General Public License does not permit incorporating your program into proprietary programs. If your program is a subroutine library, you may consider it more useful to permit linking proprietary applications with the library. If this is what you want to do, use the GNU Library General Public License instead of this License.

Microsoft Anti-Cross Site Scripting Library

Microsoft Anti-Cross Site Scripting Library v4.2.1

Copyright (c) 2010 Microsoft Corporation

Microsoft Public License (Ms-PL)

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms "reproduce," "reproduction," "derivative works," and "distribution" have the same meaning here as under U.S. copyright law. A "contribution" is the original software, or any additions or changes to the software. A "contributor" is any person

that distributes its contribution under this license. "Licensed patents" are a contributor's patent claims that read directly on its contribution.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce its contribution, prepare derivative works of its contribution, and distribute its contribution or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, each contributor grants you a non-exclusive, worldwide, royalty-free license under its licensed patents to make, have made, use, sell, offer for sale, import, and/or otherwise dispose of its contribution in the software or derivative works of the contribution in the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you rights to use any contributors' name, logo, or trademarks.

(B) If you bring a patent claim against any contributor over patents that you claim are infringed by the software, your patent license from such contributor to the software ends automatically.

(C) If you distribute any portion of the software, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(D) If you distribute any portion of the software in source code form, you may do so only under this license by including a complete copy of this license with your distribution. If you distribute any portion of the software in compiled or object code form, you may only do so under a license that complies with this license.

(E) The software is licensed "as-is." You bear the risk of using it. The contributors give no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, the contributors exclude the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

OpenPegasus

OpenPegasus v2.7.0

Copyright (c) 2000, 2001, 2002 BMC Software; Hewlett-Packard Development

// Company, L.P.; IBM Corp.; The Open Group; Tivoli Systems.

// Copyright (c) 2003 BMC Software; Hewlett-Packard Development Company, L.P.;

// IBM Corp.; EMC Corporation, The Open Group.

// Copyright (c) 2004 BMC Software; Hewlett-Packard Development Company, L.P.;

// IBM Corp.; EMC Corporation; VERITAS Software Corporation; The Open Group.

// Copyright (c) 2005 Hewlett-Packard Development Company, L.P.; IBM Corp.;

// EMC Corporation; VERITAS Software Corporation; The Open Group.

// Copyright (c) 2006 Hewlett-Packard Development Company, L.P.; IBM Corp.;

// EMC Corporation; Symantec Corporation; The Open Group.

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder" in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

OpenSSL 0.9.8u

Eric Young & Tim Hudson Copyright (c) 1998-2011.

Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

All rights reserved.

'This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)'

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/*==

*Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

* 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

* 6. Redistributions of any form whatsoever must retain the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL

DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

* This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

* This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscape SSL.

* This library is free for commercial and non-commercial use as long as the following conditions are adheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

* "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

* The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

OpenSSL 0.9.8y

Copyright (c) 1998-2011 The OpenSSL Project

Copyright (c) 1995-1998 Eric A. Young, Tim J. Hudson

All rights reserved.

'This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)'

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source

licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

OpenSSL License

/*==

*Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

* 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

* 6. Redistributions of any form whatsoever must retain the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

* This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

* This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscape SSL.

* This library is free for commercial and non-commercial use as long as the following conditions are adheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

* "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

* The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

OpenSSL 1.0.1e

Copyright (c) 1998-2011 The OpenSSL Project

Copyright (c) 1995-1998 Eric A. Young

All rights reserved.

'This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)'

This product includes software written by Tim Hudson (tjh@cryptsoft.com)

License

This is a copy of the current LICENSE file inside the CVS repository.

LICENSE ISSUES

The OpenSSL toolkit stays under a dual license, i.e. both the conditions of the OpenSSL License and the original SSLeay license apply to the toolkit. See below for the actual license texts. Actually both licenses are BSD-style Open Source licenses. In case of any license issues related to OpenSSL please contact openssl-core@openssl.org.

/*==========

*Copyright (c) 1998-2008 The OpenSSL Project. All rights reserved.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the above copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit. (http://www.openssl.org/)"

* 4. The names "OpenSSL Toolkit" and "OpenSSL Project" must not be used to endorse or promote products derived from this software without prior written permission. For written permission, please contact openssl-core@openssl.org.

* 5. Products derived from this software may not be called "OpenSSL" nor may "OpenSSL" appear in their names without prior written permission of the OpenSSL Project.

* 6. Redistributions of any form whatsoever must retain the following acknowledgment:

* "This product includes software developed by the OpenSSL Project for use in the OpenSSL Toolkit (http://www.openssl.org/)"

* THIS SOFTWARE IS PROVIDED BY THE OpenSSL PROJECT ``AS IS'' AND ANY EXPRESSED OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE OpenSSL PROJECT OR ITS CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

==========

* This product includes cryptographic software written by Eric Young (eay@cryptsoft.com). This product includes software written by Tim Hudson (tjh@cryptsoft.com).

Original SSLeay License

/* Copyright (C) 1995-1998 Eric Young (eay@cryptsoft.com)

* All rights reserved.

* This package is an SSL implementation written by Eric Young (eay@cryptsoft.com).

* The implementation was written so as to conform with Netscape SSL.

* This library is free for commercial and non-commercial use as long as the following conditions are adheared to. The following conditions apply to all code found in this distribution, be it the RC4, RSA, lhash, DES, etc., code; not just the SSL code. The SSL documentation included with this distribution is covered by the same copyright terms except that the holder is Tim Hudson (tjh@cryptsoft.com).

* Copyright remains Eric Young's, and as such any Copyright notices in the code are not to be removed.

* If this package is used in a product, Eric Young should be given attribution as the author of the parts of the library used.

* This can be in the form of a textual message at program startup or in documentation (online or textual) provided with the package.

* Redistribution and use in source and binary forms, with or without modification, are permitted provided that the following conditions are met:

* 1. Redistributions of source code must retain the copyright notice, this list of conditions and the following disclaimer.

* 2. Redistributions in binary form must reproduce the above copyright notice, this list of conditions and the following disclaimer in the documentation and/or other materials provided with the distribution.

* 3. All advertising materials mentioning features or use of this software must display the following acknowledgement:

* "This product includes cryptographic software written by Eric Young (eay@cryptsoft.com)"

* The word 'cryptographic' can be left out if the rouines from the library being used are not cryptographic related :-).

* 4. If you include any Windows specific code (or a derivative thereof) from the apps directory (application code) you must include an acknowledgement:

* "This product includes software written by Tim Hudson (tjh@cryptsoft.com)"

* THIS SOFTWARE IS PROVIDED BY ERIC YOUNG ``AS IS'' AND ANY EXPRESS OR IMPLIED WARRANTIES, INCLUDING, BUT NOT LIMITED TO, THE IMPLIED WARRANTIES OF MERCHANTABILITY AND FITNESS FOR A PARTICULAR PURPOSE ARE DISCLAIMED. IN NO EVENT SHALL THE AUTHOR OR CONTRIBUTORS BE LIABLE FOR ANY DIRECT, INDIRECT, INCIDENTAL, SPECIAL, EXEMPLARY, OR CONSEQUENTIAL DAMAGES (INCLUDING, BUT NOT LIMITED TO, PROCUREMENT OF SUBSTITUTE GOODS OR SERVICES; LOSS OF USE, DATA, OR PROFITS; OR BUSINESS INTERRUPTION) HOWEVER

CAUSED AND ON ANY THEORY OF LIABILITY, WHETHER IN CONTRACT, STRICT LIABILITY, OR TORT (INCLUDING NEGLIGENCE OR OTHERWISE) ARISING IN ANY WAY OUT OF THE USE OF THIS SOFTWARE, EVEN IF ADVISED OF THE POSSIBILITY OF SUCH DAMAGE.

* The license and distribution terms for any publically available version or derivative of this code cannot be changed. i.e. this code cannot simply be copied and put under another distribution license [including the GNU Public License.]

plists-cs

plists-cs v1.3.zip - v1.30.0

Copyright (c) 2011 Chad Burggraf

MIT License

This code is licensed under the license terms below, granted by the copyright holder listed above. The term copyright holder" in the license below means the copyright holder listed above.

Permission is hereby granted, free of charge, to any person obtaining a copy of this software and associated documentation files (the "Software"), to deal in the Software without restriction, including without limitation the rights to use, copy, modify, merge, publish, distribute, sublicense, and/or sell copies of the Software, and to permit persons to whom the Software is furnished to do so, subject to the following conditions:

The above copyright notice and this permission notice shall be included in all copies or substantial portions of the Software.

THE SOFTWARE IS PROVIDED "AS IS", WITHOUT WARRANTY OF ANY KIND, EXPRESS OR IMPLIED, INCLUDING BUT NOT LIMITED TO THE WARRANTIES OF MERCHANTABILITY, FITNESS FOR A PARTICULAR PURPOSE AND NONINFRINGEMENT. IN NO EVENT SHALL THE AUTHORS OR COPYRIGHT HOLDERS BE LIABLE FOR ANY CLAIM, DAMAGES OR OTHER LIABILITY, WHETHER IN AN ACTION OF CONTRACT, TORT OR OTHERWISE, ARISING FROM, OUT OF OR IN CONNECTION WITH THE SOFTWARE OR THE USE OR OTHER DEALINGS IN THE SOFTWARE.

SQLite

SQLite v3.3.17

This component is in the public domain.

This software is placed in the public domain. It is provided “AS IS” without warranty or support of any kind.

Windows Template Library 'WTL' v8.0

Copyright © 2007 Microsoft Corporation. All rights reserved.

Microsoft Permissive License

This license governs use of the accompanying software. If you use the software, you accept this license. If you do not accept the license, do not use the software.

1. Definitions

The terms “reproduce,” “reproduction” and “distribution” have the same meaning here as under U.S. copyright law.

“You” means the licensee of the software.

“Licensed patents” means any Microsoft patent claims which read directly on the software as distributed by Microsoft under this license.

2. Grant of Rights

(A) Copyright Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, Microsoft grants you a non-exclusive, worldwide, royalty-free copyright license to reproduce the software, prepare derivative works of the software and distribute the software or any derivative works that you create.

(B) Patent Grant- Subject to the terms of this license, including the license conditions and limitations in section 3, Microsoft grants you a non-exclusive, worldwide, royalty-free patent license under licensed patents to make, have made, use, practice, sell, and offer for sale, and/or otherwise dispose of the software or derivative works of the software.

3. Conditions and Limitations

(A) No Trademark License- This license does not grant you any rights to use Microsoft’s name, logo, or trademarks.

(B) Platform Limitation- The licenses granted in sections 2(A) & 2(B) extend only to the software or derivative works that you create that run on a Microsoft Windows operating system product.

(C) If you begin patent litigation against Microsoft over patents that you think may apply to the software (including a cross-claim or counterclaim in a lawsuit), your license to the software ends automatically.

(D) If you distribute copies of the software or derivative works, you must retain all copyright, patent, trademark, and attribution notices that are present in the software.

(E) If you distribute the software or derivative works in source code form you may do so only under this license (i.e., you must include a complete copy of this license with your distribution), and if you distribute the software or derivative works in compiled or object code form you may only do so under a license that complies with this license.

(F) The software is licensed “as-is.” You bear the risk of using it. Microsoft gives no express warranties, guarantees or conditions. You may have additional consumer rights under your local laws which this license cannot change. To the extent permitted under your local laws, Microsoft excludes the implied warranties of merchantability, fitness for a particular purpose and non-infringement.

Zlib

Copyright (C) 1995-2010 Jean-loup Gailly and Mark Adler

zlib/libpng License

This software is provided 'as-is', without any express or implied warranty. In no event will the authors be held liable for any damages arising from the use of this software.

Permission is granted to anyone to use this software for any purpose, including commercial applications, and to alter it and redistribute it freely, subject to the following restrictions:

1. The origin of this software must not be misrepresented; you must not claim that you wrote the original software. If you use this software in a product, an acknowledgment in the product documentation would be appreciated but is not required.

2. Altered source versions must be plainly marked as such, and must not be misrepresented as being the original software.

3. This notice may not be removed or altered from any source distribution.

Index

A

Abfrage filtern
- Abfrageergebnisse anzeigen 564
- Anzeigen der gelösten Abfrage 563
- Hinzufügen von Filter-Ausdrücken zur Abfrage 560
- Info 478
- Konvertieren einer Ressourcen-Abfrage in eine SQL-Abfrage 478
- Quellfelder, SQL-Abfrage 558
- Schreiben einer SQL-Abfrage 558

Abfragegenerator
- Verwenden für Filterabfrage 374

Active Directory Import
- Computer erkennen 207
- Import-Updates 212
- Ressourceimporte planen 212
- Volle Importe 212
- Zu verwendender Prozess 207

Active Directory, Import
- Berichte 205
- Fehlerprotokoll 205
- Info 205
- Ressourcenimportregeln 209
- Ressourcentypen unterstützt 209

Active Directory-Import
- Ressourcenerkennung 198
- Ressourcenimporte manuell ausführen 214
- Ressourcenzuordnungen, importieren 206
- Verzeichnissynchronisierung, Zeitplan 213

AeXGenClientCert.exe
- Kommandozeilenparameter 343
- Überblick 538

AeXGenSiteServerCert.exe
- Kommandozeilenparameter 309
- Überblick 538

AeXNSAgent.exe
- Kommandozeilen-Switches 545

AeXRevokeCertificate.exe
- Kommandozeilenparameter 347
- Überblick 538

Agent. *Siehe* Symantec Management-Agent

Agent verteilen 189

Agent- und Aufgabeneinstellungen
- Automatische Optimierung 192
- Optimierung 192

Agent-Einstellungen
- Automatische Optimierung 189
- Optimierung 189

Agent-Registrierungsanforderung
- blockieren 261
- zulassen 261

Agent-Registrierungseinträge
- Bereinigen 82

Agent-Registrierungsrichtlinie
- erstellen 253

Agent-Registrierungsstatus
- Bericht 261

Agent-Vertrauen
- akzeptieren 253
- aufbauen 247
- blockieren 253
- Info zu 247
- Registrierungsrichtlinie 253
- widerrufen 261

Aggregation
- Typen 576

Aktualisierungszeitplan fertig stellen
- Konfigurieren 384

Anforderungen
- Symantec Management-Agent installieren 252

Ansicht "Computer"
- Info zu 36

Ansicht "Software"
- Info 41

Anwendungsidentität
- Notification Server 69

Archivieren
- Aufgabendaten 449

archivieren
- Aufgabenversionsdaten 450

ARP 224

Aufgabe
abhängig von Filter 382
Änderung für Automatisierungsrichtlinie 423
Anzeigen auf internem Zeitplankalender 130
Ausführen 442
Automatisierungsrichtlinie, Aktion 421
Eingabeparameter festlegen 421
erstellen 438
Erstellung für Automatisierungsrichtlinie 423
für Automatisierungsrichtlinie auswählen 423
Planen 444
sequenzieren 436
Verwendung 432
Ziel, festlegen 396
Aufgabe "Network Discovery"
Erstellen 220
Ort 220
Aufgabe "Netzwerksuche"
ändern 221
Erstellen 221
Ort 221
Protokolleinstellungen 222
Verbindungsprofil 222
Aufgabe, Eingabe
erhalten 446
Aufgabendaten
bereinigen 449
Aufgabenstatusinformationen
Hierarchie 433
Aufgabenversionsdaten
bereinigen 450
Auftrag
Planen 444
Aufträge und Aufgaben
ausführen 441
Ausdruck
Operatoren 575
Syntax 574
Ausführliches Protokoll
bereinigen 508
ausgeführte Aufgaben
Hierarchie 433
Automatische Optimierung
Agent- und Aufgabeneinstellungen 192
Automatische Optimierung von Agent-Einstellungen 189
Automatisierungsrichtlinie
Aktion 409
Aktion festlegen 421
Aktionen ausführen aus 411
Aktivierung und Deaktivierung 411
Ändern von Aufgaben 423
Angeben der Datenquelle 419
Anzeigen auf internem Zeitplankalender 130
Auslöser 409
Auswertungsregel 409
Auswertungsregel einrichten 414, 416
Datenquelle 409
Erstellen von Aufgaben 423
geplante ändern 414
geplante erstellen 414
Info 408
Komponenten 409
Löschen 411
meldungsabhängige Änderung 416
meldungsabhängige Erstellung 416
Sicherheit einstellen auf 411
testen 411
Verwalten 411
Automatisierungsrichtlinien
Hierarchie 176

B

Benutzer
Benutzerbasierte Richtlinien 394
Benutzerbericht. *Siehe* Benutzerdefinierter Bericht
Benutzerdefiniert
Werte 575
benutzerdefinierte Suchkriterien
erstellen 39, 41
Benutzerdefinierter Bericht
Abfrage 478
Siehe auch Berichtsabfrage
Abfrageergebnisse anzeigen 564
Abfrageparameter
Info 559
Ändern 478
Anzeigen der gelösten Abfrage 563
Bearbeiten 473
Berichtparameter
Ändern 481
Einstellungen 571
erstellen 481
Hinzufügen 481
Hinzufügen des erweiterten Typs 481
Berichtsparameter, definieren 481
Diagrammansicht, Info 483
Siehe auch Diagrammansicht, Bericht

Drilldown, Ergebnisse 486
Drilldown-Aktion, festlegen 486
Drilldown-Aktion, Info 486
Drilldown-Aktion, Parameter 486
Drilldown-Aktion, Wireup 486
Eigenschaften, festlegen 489
Erstellen 473
erstellen 476
Erstellen einer Ressourcenabfrage 553
Hinzufügen von Filter-Ausdrücken zur Abfrage 560
Info 473
Komponenten 471
Konvertieren einer Ressourcen-Abfrage in eine SQL-Abfrage 478
Quellfelder
bearbeiten 570
zur Ressourcenabfrage hinzufügen 557
Quellfelder, SQL-Abfrage 558
Rasteransicht, Info 485
Siehe auch Rasteransicht, Bericht
Ressourcenabfrage 478
Schreiben einer SQL-Abfrage 558
SQL-Abfrage 480
Benutzerkonto
Allgemeine Kontodetails 101
Einstellen der Berechtigungs-Vererbungsregeln für Ordner 109
Erstellen 97
Gesperrte Identifikationsdaten freigeben 118
Kennwortkomplexitätseinstellungen 115
Kennwortsperreinstellungen 115
Konfigurieren 97
Sicherheitsrollen zuweisen 106
Benutzerspezifische Anpassung
Konsolenmenü 54
Berechtigungen
Anzeige 119
Berechtigung, Kategorien 512
Berichte 529
Credential Manager 531
Der Sicherheitsrolle zuweisen 108
Filter 530
Info 512
Ordner 529
Ressourcenverwaltung 527
Richtlinien 529
System 528
Task Server 528
Verbindungsprofile 530
Bereinigen
Aufgabendaten 449
bereinigen
Aufgabenversionsdaten 450
Bericht
Aktionen für Ergebniselemente durchführen 465
als Web-Part speichern 469
ändern. *Siehe* Benutzerdefinierter Bericht
Anzeigen von Ergebnissen 464
Benutzerparameter angeben 462
benutzerspezifische Anpassung. *Siehe* Benutzerdefinierter Bericht
Datenquelle für Automatisierungsrichtlinie 419
Diagrammansicht auswählen 464
Drilldown, Ergebnisse 465
Ergebnisse als statischer Filter speichern 467
Ergebnisse drucken 465
Ergebnisse extrahieren 462
erstellen. *Siehe* Benutzerdefinierter Bericht
Hierarchieberichte 177
Info 460
Rasteransicht auswählen 464
Snapshot speichern 468
Snapshots auswählen 462
Speichern von Ergebnissen in einer Datei 466
Symantec Management-Agent-Installationsstatus 260
Verwendung 461
Berichtabfrage
Ressourcenabfrage 478
Berichte
Cloud-fähige Verwaltung 353
Berichtsabfrage
Abfrageergebnisse anzeigen 564
Abfrageparameter
Info 559
Anzeigen der gelösten Abfrage 563
Bereichsdefinition, Daten-Snapshot 560
Berichtparameter
Ändern 481
Einstellungen 571
erstellen 481
Hinzufügen 481
Hinzufügen des erweiterten Typs 481
Berichtsparameter, definieren 481
Erstellen einer Ressourcenabfrage 553
Hinzufügen von Filter-Ausdrücken zur Abfrage 560

Info 478
Konvertieren einer Ressourcen-Abfrage in eine SQL-Abfrage 478
Quellfelder
bearbeiten 570
zur Ressourcenabfrage hinzufügen 557
Quellfelder, SQL-Abfrage 558
Schreiben einer SQL-Abfrage 558
SQL-Abfrage 480
Berichtsdaten-Snapshot
Bereinigen 82

C

CEM-Agent-Einstellungen
konfigurieren 324
CEM-Agent-IIS-Website
Einstellungen 324
CEM-Zertifikat
widerrufen 347
Client Task Agent
Einstellungen 451
Clientzertifikat
Generieren mit AeXGenClientCert.exe 343
Cloud-fähige Verwaltung
Agent-Installationspaket, generieren 544
Agent-Installationspaket, Parameter 544
Berichte 353
erforderliche Aktivitäten 300
Gemischte Umgebung 539
Info zu 297
Internet-Gateway 321
Kommandozeilen-Switches "AeXNSAgent.exe" 545
Kommandozeilenprogramme 538
Konfigurieren der Einstellungsrichtlinie für die Cloud-fähige Verwaltung 334
Package Server 540
Site Server 540
Task Server 540
Vorbereiten der Site Server 300
Vorbereiten der Umgebung 300
Widerrufen des Zertifikats 347
Cloud-fähige Verwaltung - Einstellungsrichtlinie
deaktivieren 334
Cloud-fähige Verwaltung – Einstellungsrichtlinie
aktivieren 334
konfigurieren 334
Cloud-fähiger Agent
auf nicht verbundenem Computer installieren 338
Clientzertifikat entfernen 346
Fehlerbehebung 342
Internet-Gateway-Auswahl, erzwingen 350
Kommandozeilen-Switches 545
Temporäres Clientzertifikat installieren 346
CMDB
Alte Daten bereinigen 82
Befehls-Timeout 78
Datenbankname 78
Identifikationsdaten für Datenbankzugriff 78
Info 78
Konfigurieren 78
Name des Datenbankservers 78
öffentlicher Bericht, Identifikationsdaten 78
Ressourcendatenverlauf 84
SQL-Authentifizierung 78
Windows-Authentifizierung 78
CMDB-Daten
bearbeiten 505
CMDB-Regel
als Aufgabe ausführen 506
CMDB-Regeln
Info 505
Computer
Anforderungen für das Installieren des Symantec Management-Agent 252
Erkennen 186
Erkennungsmethoden 199
für Symantec Management-Agent-Installation auswählen 256
geplante Symantec Management-Agent-Installation 259
globale Agent-Einstellungen 290
Info zum Erkennen 199
Konfigurieren von Wartungsfenstern 292
mit Active Directory-Import erkennen 207
mit Ressourcenerkennung erkennen 200
nach suchen 39
Pull-Installation von Symantec Management-Agent für UNIX, Linux und Mac 276
Push-Installation von Symantec Management-Agent 256
Push-Installation von Symantec Management-Agent für UNIX, Linux und Mac 272
Suchen 45
Symantec Management-Agent 246
Symantec Management-Agent installieren 248

Symantec Management-Agent manuell deinstallieren 286
Symantec Management-Agent manuell installieren 250, 266
Symantec Management-Agent – Pull-Installation 258
Symantec Management-Agent-Aktualisierungsrichtlinie 280
Symantec Management-Agent-Datenaktualisierungsabstände 532
Symantec Management-Agent-Deinstallationsrichtlinie 280
Symantec Management-Agent-Richtlinien konfigurieren 288
Wartungsfenster 292
Ziel-Agent-Einstellungen 290
Computer erkennen 186
Computerbericht. *Siehe* Benutzerdefinierter Bericht
Computerdaten
Bereinigen 82
Computersuche
als Filter speichern 39
ausführen 39
Configuration Management Database. *Siehe* CMDB
Credential Manager
Info 121
CSV-Datei
Berichtergebnisse speichern 466
Computer importieren 256

D

Data Connector
Einsatzmöglichkeiten 497
Funktionen 497
Funktionsweise 495
Info 495
Daten
vorbereiten 500
Datenklasse
Ereignisdaten anzeigen 456
Inventardaten anzeigen 456
Virtuell 507
Datenquelle
Angabe für Automatisierungsrichtlinie 419
Definition erstellen 500
Verwenden einer SQL-Abfrage für eine Automatisierungsrichtlinie 419
Verwendung einer Meldung für eine Automatisierungsrichtlinie 419
Verwendung einer Ressourcenabfrage für eine Automatisierungsrichtlinie 419
Verwendung eines Berichts für eine Automatisierungsrichtlinie 419
Datenquellendefinition
Erstellen 500
Datensynchronisierung
Hierarchieanforderungen 162
Hierarchiereplikation 170
Hierarchiereplikation manuell ausführen 174
Notification Server-Hierarchie 160
Replikationsanforderungen 182
zwischen Notification Servern replizieren 180
Datenübertragung
Einrichten 498
Konfigurieren 501
Übersichten 504
Datenübertragungsregel
ausführen 503
Prüfen 504
DefaultAppPool
einstellen 324
Delta-Aktualisierungszeitplan
Konfigurieren 384
Diagrammansicht, Bericht
3D-Zoom 565
Ändern 483
Diagrammlegende 565
Diagrammtitel 565
Einstellungen für X-Achse 565
Einstellungen für Y-Achse 565
Erstellen 483
Info 483
Dokumentation 30
Aufrufen 50
Domänenmitgliedschaft
Ressourcenerkennung 198
Drag & Drop
Aufträge und Aufgaben ausführen 441
Drag and Drop
Richtlinie anwenden 395

E

E-Mail-Benachrichtigungen
Konfigurieren 73
Eigenschaften
Eingabe 446
Eingabeeigenschaften
erhalten 446

Eingabeparameter
erhalten 446
Einstellungen
Client Task Agent 451
Task Server 451
Element
Berechtigungen festlegen 108
in Besitz nehmen 120
Ereignisdaten
Anzeigen 456
Erkennen von Netzwerkgeräten 217
Erkennung
Active Directory-Import 198
Domänenmitgliedschaft 198
Network Discovery 198
Netzwerkgeräte 216
Ressourcen 198
Ersteinrichtung
Patch-Management 195
Erstellen und Ausführen von Network Discovery-Aufgaben
Symantec Vorgesetzten es ermöglichen 235
Erstmaliges Setup
Portal 185
Erweiterte Ansichten
Ansicht "Computer" 36
Info zu 36, 41
erweiterte Ansichten
Aufträge und Aufgaben ausführen 441
Einstellungen 46
Richtlinie anwenden 395
Softwareansicht 41
Evaluierung
Lizenz 29
Exportieren von Daten 498
Exportregel
Erstellen 501

F

Filter
Abfrage 478
Siehe auch Abfrage filtern
Abfragetyp auswählen 373
Abhängigkeiten 382
Aktionen für Ressourcen durchführen 381
Ändern 372
Ausschlüsse 378
Einschlüsse 378
Erstellen 372
Info 369
Kontextmenü für Mitglieder 381
Mitgliedschaft aktualisieren 380
Mitgliedschaftsaktualisierungen planen 384
Prozess zum Erstellen 370
Ressourcenabfrage 374
SQL-Abfrage 377
statischen Filter aus Berichtergebnissen erstellen 467
Filterabfrage
Abfrageparameter
Info 559
Filtern der Abfrage
Erstellen einer Ressourcenabfrage 553
Funktion
Ausdruck 576
Convert 577
IIF 578
IsNull 578
Len 577
Substring 579
Trim 579

G

Gemeinsam genutzter Zeitplan
aktivieren 128
ändern 128
Anzeigen auf internem Zeitplankalender 130
Anzeigen der Zeitplan-Benutzer 128
Erstellen 128
Info 128
Löschen 128
Geräteerkennung 216
gespeicherte Suchvorgänge
verwalten 41

H

Hierarchie
Anforderungen 162
Aufgabenstatusinformationen 433
ausgeführte Aufgaben 433
Automatisierungsrichtlinien 176
Automatisierungsrichtlinien ausführen 176
Berichte 177
Einrichten 163
Entfernen eines Notification Servers 164
Hierarchiebeziehungen ändern 168
Hierarchiebeziehungen erstellen 168

hierarchische Beziehungen erstellen 164
Info 160
manuelles Replizieren ausgewählter Daten 175
Replikation. *Siehe* Hierarchiereplikation
Replikation aktivieren 164
Warnstatusanzeige 164
Hierarchieberichte
Aktualisieren von Übersichtsdaten 178
Hierarchiereplikation
benutzerdefinierte Replikation 173
Differenzial-Replikationszeitplan überschreiben 174
differenzielle Replikation 170
Elemente 170
Konfigurieren 170
manuelles Replizieren ausgewählter Daten 175
Replizierungsregeln 170
Ressourcen 170
Sicherheitsobjekte 170
vollständige Replikation 170
Hilfe
Aufrufen 50
Kontextbezogen 30
HTML-Datei
Berichtergebnisse speichern 466
HTTPS-Konfiguration
auf verwaltetem Computer 305

I

ICMP-Einstellungen
Aufgabe "Netzwerksuche" 222
Identifikationsdaten
Bearbeiten 121
Erstellen 121
IIS-Website
konfigurieren 324
Importieren von Daten 498
Importregel
Erstellen 501
Installationseinstellungen
Symantec Management-Agent für UNIX, Linux und Mac 271
Internet-Gateway
Auswahl auf Cloud-fähigem Agent erzwingen 350
Certificate Revocation List anwenden, Skript 542
einrichten 321
Hostcomputer konfigurieren 327
Installationspaket ausführen 329
Installationspaket herunterladen 329
installieren 321
Internet-Gateway-Dienst anhalten, Skript 542
Internet-Gateway-Dienst registrieren, Skript 542
Internet-Gateway-Dienst starten, Skript 542
Internet-Gateway-Dienst-Registrierung aufheben, Skript 542
Konfigurationsdateien 321
Konfigurieren 331
Lastverteilung 543
Notification Server-Zertifikat anwenden, Skript 542
Port 331
Protokolldateien 321
Serverzertifikat neu generieren, Skript 542
Sichern 351
Teilweise Wiederherstellung 351
Überblick 321
Verwalten 542
Vollständige Wiederherstellung 351
vorbereiten 327
IT Management Suite 7.5
Neue Funktionen 24

J

Jetzt bereinigen 82
Job
Ausführen 442
erstellen 439
sequenzieren 436
Verwendung 432
Job- und Aufgabenportal
Zugriff 452
Jobs- und Aufgabenansicht
Info 44

K

Kommandozeilentool
AeXGenClientCert.exe 538
AeXGenSiteServerCert.exe 538
AeXRevokeCertificate.exe 538
Konfiguration
Erstmalige Produktinstallation 185
Konfigurationseinstellungen
Konfigurieren mit NS Configurator 77
Konsole. *Siehe* Symantec Management Console
Konsolenansicht
ändern 57
Elementverknüpfungen hinzufügen 58

erstellen 57
Info 35
Komponenten hinzufügen 58
Verzeichnisstruktur, überschreiben 35
Weblinks hinzufügen 58
Konsolenmenü
benutzerspezifische Anpassung 54
Menüelemente hinzufügen 54
Untermenü aus XML-Datei importieren 54
Untermenüs hinzufügen 54
Kontextbezogene Hilfe 30
Kontextmenü
Festlegen von Ersatzparametern 55
Hinzufügen der Kommandozeile 55
Hinzufügen einer benutzerdefinierten Aktion 55
Hinzufügen einer URL 55
mit Filtermitgliedern verwenden 381

L

Legacy-Agent-Kommunikation
Aktivieren 69
aktivieren 284
Deaktivieren 69
deaktivieren 284
Info zu 284
Standardstatus 284
Legacy-Berichtsdaten
Bereinigen 82
Lizenz
Evaluierung 29
Lösungen 29
Löschen
Aufgabendaten 449
löschen
Aufgabenversionsdaten 450
Lösungen
Installieren 29
Lizenz 29
Lösungs-Agent
Deinstallationsrichtlinie 406
Installationsrichtlinie 406
Upgrade-Richtlinie 406

M

Manuelles Installieren des Symantec Management-Agent
Computer auswählen 256
Maximale Thread-Zahl
Network Discovery 218
Mein Portal (Seite)
Info 51
Meldung
Datenquelle für Automatisierungsrichtlinie 419
Menüelement
exportieren 54
Hinzufügen zum Konsolenmenü 54
importieren 54
MIB-Dateien
importieren 243

N

nach einem Computer suchen 39
Limits konfigurieren 46
Suchfeldeinstellungen 46
Nach einer Software suchen 45
nach einer Software suchen 41
Limits konfigurieren 46
Suchfeldeinstellungen 46
Network Discovery 216–217, 220–221
Assistent 217
Aufgabe 221
Aufgaben delegieren 229, 233, 238, 240, 242
Berichte 227
Einstellungen 218
Ergebnisse 227
Erkennungsaufgaben delegieren 240
Info 198
Konfiguration 218
maximale Thread-Zahl 218
Methoden 224
Netzwerkbereich auswählen 226
Prozess für die Delegierung von Aufgaben 229
Vorgang 217
Network Discovery-Assistent 220
Network Discovery-Aufgaben
delegieren 235
Symantec Vorgesetzten das Erstellen ermöglichen 235
Netzwerkgeräte
andere Benutzer erkennen lassen 229
Erkennungsaufgaben delegieren 229, 233, 235, 238, 242
Notification Server
Anwendungsidentität 69
Configuration Management Database 78
E-Mail-Adresseinstellungen 73

Filter. *Siehe* Filter
Funktionen 66
für Cloud-fähige Verwaltung konfigurieren 315
für die Verwendung von HTTPS konfigurieren 300
Für HTTPS konfigurieren 304
Gemeinsam genutzte Zeitpläne 128
Hierarchie 160
hierarchische Beziehungen erstellen 164, 168
Info 66
Interner Zeitplankalender 130
Konfiguration, Überblick 67
Konfigurationseinstellungen, Übersicht 68
Konfigurationstypen 67
Konfigurationsverfahren 68
Konfigurieren mit NS Configurator 77
NSE-Verarbeitung 69
Siehe auch NSE-Verarbeitung
Package Server 145
Siehe auch Package Service
Protokolldatei anzeigen 74
Proxy-Server-Konfiguration 76
Replikation 180
Richtlinien. *Siehe* Richtlinie
Site. *Siehe* Services
Site Server. *Siehe* Site Server
Site Services 133, 145
Siehe auch Site Service
Statusmeldung, Protokollierung 74
Statusmeldungen anzeigen 74
Subnetz. *Siehe* Subnetz
Überblick 27
Verarbeitungseinstellungen 69
Zeitpläne 125
Siehe auch Zeitplan
Zeitplanverwendung 123
Notification Server-Hierarchie. *Siehe* Hierarchie
Notification Server-Replikation. *Siehe* Replikation
Notification Server-Ressourcen. *Siehe* Ressourcen
Notification Server-Zertifikat
auf verwalteten Computer anwenden 305
von Notification Server exportieren 305
NS Configurator
Info 77
NSE-Verarbeitung
Konfigurationseinstellungen 69
manuell aktivieren 69

O

Optimieren von Agent-Einstellungen 189
Optimierung
Agent- und Aufgabeneinstellungen 192
Ordner
Berechtigungen festlegen 108
Einstellen der Berechtigungs-Vererbungsregeln 109
in Besitz nehmen 120
Organisationsansicht
Ändern 358
Erstellen 358
Filtergruppen 358
Info 358
Standardansicht 358
Verwendung in der Ressourcensicherheit 355
Organisationsansichten
Erkannte Geräte anzeigen 227
Organisationsansichten und Gruppen
auffüllen 359
erstellen 359
Organisationsgruppe
Aktionen für Mitglieder durchführen 361
Benutzer hinzufügen 360
Benutzerdefinierte Sicherheitsberechtigungen festlegen 362
Computer hinzufügen 360
Gruppe bearbeiten 360
Info 360
Ressource hinzufügen 457
Ressourcen anzeigen 361
Ressourcen hinzufügen 360
Ressourcenverwaltungsberechtigungen festlegen 362
Systemberechtigungen festlegen 362
Task Server-Berechtigungen festlegen 362
verwalten 361
Verwendung in der Ressourcensicherheit 355
Zeitplan aktualisieren 384
Zuweisen von Sicherheitsrollen 362

P

Package Server
für Cloud-fähige Verwaltung konfigurieren 315
HTTPS-Codebasen veröffentlichen 315
Konfigurationen 539
Package Server für Linux 148
Apache Web Server erkennen 150
Info zur 148

Info zur Integration von Apache Web Server 149
Info zur Konfiguration von Apache Web Server 152
Info zur Konfiguration von HTTPS und HTTP 153
Konfigurationsbeispiele 154
Unterstützte Plattformen 148
Package Service
Einstellen als "Uneingeschränkt" 146
Einstellungen konfigurieren 146
Paket
Symantec Management-Agent 286
Paketverteilungspunkte
Aktualisierung 388
Identifikationsdaten angeben 76
Parameter
Eingabe 446
Patch-Management
planen 195
pcAnywhere Solution
Funktionen 28
Komponenten 28
Ping 224
Planen
Anwenden auf Richtlinie 404
Platzhalter
Zeichen 576
Portalseite
ändern 59
erstellen 59
Info 59
Mein Portal 59
Notification Server Management – Startseite 51
Privileg, Sicherheit
Asset-Status, Element 527
benutzerdefinierte Hierarchiereplikation 173
Connector-Beispiele 524
Hierarchie 524
Kategorien 510
Lösungsspezifische Aktion 525
Rechtsklickaktion 522
Softwaremanagementaktion 525
Verwaltung 514
Problemlösung 533
Problemlösung in der Kommandozeile 533
Protokoll
öffnen 74
Protokolleinstellungen
Aufgabe "Netzwerksuche" 222
Proxy-Server
Konfigurieren 76

R

Rasteransicht, Bericht
ändern 485
erstellen 485
Erweiterte Formatierung 568
Formatierungsbedingungen 568
Formatierungsvorlage 568
Info 485
Recht, Sicherheit
Der Sicherheitsrolle zuweisen 97
Identifikationsdaten 518
Symantec Management Console 519
System 516
Verbindungsprofil 513
Workflow-Verzeichnis 519
Replikation
Anforderungen 182
differenzielle 180
Elemente 183
Ereignisse 183
Hierarchie. *Siehe* Hierarchiereplikation
Info 180
Konfigurieren 183
Replikationsregeln 183
Replizierungsregeln aktivieren 183
Replizierungsregeln ausführen 183
Replizierungsregeln erstellen 183
Replizierungsregeln löschen 183
Ressourcen 183
Sicherheit 183
vollständig(e) 180
Replikationsregeln
Replikation 183
Replizierungsregeln
Hierarchiereplikation 170
Ressource
Zu Organisationsgruppe hinzufügen 457
Ressourcen
Aktionen für Filtermitglieder durchführen 381
aus Filter ausschließen 378
Datenklasseninformationen anzeigen 492
Filtermitgliedschaftsaktualisierungen 380
geplante Filteraktualisierungen 384
in Filter einschließen 378
Info 491
mit einem Filter auswählen 369

Ressourcentypinformationen anzeigen 492
Ressourcenzuordnungstypinformationen anzeigen 492
Sicherheit. *Siehe* Ressourcensicherheit
Ressourcen mit Bereichsfestlegung
Filter 364
Info zu 364
Kurzanleitung 364
Organisationsansichten 364
Ziele 364
Ressourcen-Suchschlüssel
Erstellen 502
Ressourcenabfrage
Abfrageergebnisse anzeigen 564
Abfrageparameter
Info 559
Anzeigen der gelösten Abfrage 563
Berichtparameter
Ändern 481
Einstellungen 571
erstellen 481
Hinzufügen 481
Hinzufügen des erweiterten Typs 481
Berichtsparameter, definieren 481
Datenquelle für Automatisierungsrichtlinie 419
Definieren für Filter 374
Erstellen mit dem Abfragegenerator 553
Hinzufügen von Filter-Ausdrücken zur Abfrage 560
Quellfelder
bearbeiten 570
hinzufügen 557
Ressourcenbericht. *Siehe* Benutzerdefinierter Bericht
Ressourcendaten
Anzeigen 456
Ressourcendatenverlauf
Speichern in der CMDB 84
Ressourcenereignisdaten
Bereinigen 82
Ressourcenerkennung
Active Directory-Import 198
Computer erkennen mit 200
Domänenmitgliedschaft 198
Info 198
Network Discovery 198
Ressourcenfilter. *Siehe* Filter
Ressourcenmanager
Aufgaben 457
Daten anzeigen 456
Ereignisdaten anzeigen 456
Info 454
Ressource hinzufügen 457
von Berichtergebnissen öffnen 465
Zugreifen 455
Ressourcensicherheit
Benutzerdefinierte Sicherheitsberechtigungen für Organisationsgruppe festlegen 362
Einstellen der Sicherheit der Organisationsgruppe 362
Info 355
Konfigurieren 355
Organisationsansichten 358
Organisationsgruppen 360
Ressourcenverwaltung. *Siehe* Ressourcenmanager
Ressourcenziel. *Siehe* Ziel
Richtlinie
abhängig von Filter 382
Agent-Deinstallation 406
Agent-Installation 406
Agent-Upgrade 406
anwenden 395
Anzeigen auf internem Zeitplankalender 130
Automatisierungsrichtlinien 408
Siehe auch Automatisierungsrichtlinie
Automatisierungsrichtlinien für die Hierarchie 176
Benutzerbasiert 394
geplante Automatisierungsrichtlinie 414
globale Agent-Einstellungen 290
Info 393
meldungsabhängige Automatisierungsrichtlinie 416
Planen 404, 444
Richtlinienansicht 395
Symantec Management-Agent aktualisieren 280
Symantec Management-Agent deinstallieren 280
Typen 393
verwalten 395
Verwendung von Aufgaben und Jobs 432
Wartungsfensterrichtlinie 292
Ziel 383
Ziel, festlegen 396
Ziel-Agent-Einstellungen 290
Richtlinienaktualisierungszeitplan
Konfigurieren 384
Richtlinienansicht
Info 44

S

Seite zum Bearbeiten von benutzerdefinierten Berichten
  Ansichten (Registerkarte) 565, 568
Sequenzieren
  Aufgaben 436
Serververarbeitung
  Konfigurationseinstellungen 69
Serverzertifikat
  Anwenden auf Site Server 309
  Generieren mit AeXGenSiteServerCert.exe 309
Sicherheit
  Einrichten 88
  Gesperrte Identifikationsdaten freigeben 118
  Info 86
  Kennwortkomplexitätseinstellungen 115
  Kennwortsperreinstellungen 115
  Ressourcen. *Siehe* Ressourcensicherheit
  Standardrollen 112
  Verwalten 114
  Vordefinierte Rollen 112
Sicherheitsrolle
  Asset-Status, Elementprivilegien 527
  Benutzerdefinierte Berechtigungen für Organisationsgruppe festlegen 362
  benutzerdefinierte Hierarchiereplikation 173
  Berechtigungen zuweisen 108
  Connector-Beispiele, Privilegien 524
  Einstellen der Berechtigungs-Vererbungsregeln für Ordner 109
  Elementaufgaben-Privilegien 522
  Hierarchie-Privilegien 524
  Identifikationsdaten-Privilegien 518
  Mitglieder hinzufügen 105
  Ordner oder Element in Besitz nehmen 120
  Organisationsgruppen zuweisen 362
  Privilegien zuweisen 97
  Privilegkategorien 510
  Rechtsklickaktions-Privilegien 522
  Ressourcensicherheit 355
  Softwaremanagementaktion, Privilegien 525
  Standard 112
  Symantec Management Console-Rechte 519
  Systemrechte 516
  Verbindungsprofil-Privilegien 513
  Verwaltungsprivilegien 514
  Vordefiniert 112
  Workflow-Verzeichnisprivilegien 519
  Zuweisen als Mitglied anderer Rollen 107
Sicherheitsrollen
  Erstellen 91
  Info 91
  Konfigurieren 91
Sicherheitsrollenmanager
  Info zu 119
  Zugreifen 119
Site
  Ändern 135
  Erstellen 135
  für Cloud-fähige Agents konfigurieren 317
  Site Services 133
  Verwalten 135
Site Server
  aus Standort entfernen 137
  einer Site zuweisen 317
  erstellen 137
  für Cloud-fähige Agents konfigurieren 317
  manuell zum Standort zuweisen 140
  Site Services entfernen 137
  Site Services hinzufügen 137
  Status 137
  verwalten 137
  Zertifikat installieren 309
Site Service
  Einstellungen konfigurieren 145
Site-Server
  ändern 137
Skriptfähige Felder
  Substring 573
Snapshot
  aus Berichtergebnissen erstellen 468
SNMP-Einstellungen
  Aufgabe "Netzwerksuche" 222
SNMP-Geräte
  Klassifizieren 228
SNMP-Geräteklassifikation 218
Software
  Suchen 45
  suchen 41
Software Management Framework
  Info 27
Softwarekatalog, Fenster
  Info 43
Softwarepaket
  Aktivieren des Zugriffs mithilfe des UNC-Pfads 389
  Konfigurationseinstellungen 387
  Programm entfernen 390

Programm hinzufügen 390
Programme verwalten 390
Verteilungspunkte aktualisieren 387–388
Softwaresuche
ausführen 41
speichern 41
Softwareupdates
Download planen 195
installieren 195
Sperrzeitraum
Anzeigen auf internem Zeitplankalender 130
SQL-Abfrage
Abfrageergebnisse anzeigen 564
Abfrageparameter
Info 559
Anzeigen der gelösten Abfrage 563
Bereichsdefinition, Bericht-Snapshots 560
Berichtparameter
Ändern 481
Einstellungen 571
erstellen 481
Hinzufügen 481
Hinzufügen des erweiterten Typs 481
Berichtsparameter, definieren 481
Daten-Snapshot 560
Datenquelle für Automatisierungsrichtlinie 419
Einsetzen von Quellfeldern 558
für Filter definieren 377
Schreiben 558
SQL-Bericht. *Siehe* Benutzerdefinierter Bericht
Standort
Agents manuell zuweisen 141
löschen 135
Site Server 134
Site Server entfernen 135
Site Server manuell zuweisen 140
Standortwartung 134
Subnetz entfernen 135
Subnetz zuweisen 142
Uneingeschränkter Package Server 146
Statischer Filter
aus Berichtergebnissen erstellen 467
Statusmeldungen
im Protokoll anzeigen 74
Protokollierung 74
Subnetz
löschen 142
Neusynchronisierung 142
Verwalten 142
zu Standort zuweisen 142
Suchen nach einem Computer 45
Suchoperatoren
Info 45
Symantec Management Agent
deinstallieren 280
Symantec Management Console
Anpassbare Komponenten 52
Anpassen 33, 52
anzeigen. *Siehe* Konsolenansicht
aufrufen 48
Dokumentation 50
Elemente als XML-Dateien speichern 63
Hilfe 50
Info 33
lokaler Zugriff 48
Menü. *Siehe* Konsolenmenü
Menü aus XML-Datei importieren 54
Portalseite. *Siehe* Portalseite
Remote-Zugriff 48
Startseite 51
Untermenü als XML-Datei speichern 54
Web-Part. *Siehe* Web-Part
Symantec Management-Agent
Aktualisieren 278
Aktualisierungsmethoden 278
Anforderungen 252
auf nicht verbundenem Computer installieren, Prozess 338
Computer aus CSV-Datei importieren 256
Computer für Installation auswählen 256
Datenaktualisierungsintervalle 532
Deinstallationsrichtlinie 280, 406
Fehlerbehebung für Cloud-fähige Verwaltung 342
Für die Verwendung von HTTPS umleiten 308
für die Verwendung von HTTPS umleiten 300
geplante Installation 259
globale Einstellungen 290
Info 246
Installationsanforderungen 252
Installationsmethoden 248
Installationsstatusbericht 260
Installieren auf ausgewählten Windows-Computern 256
Konfigurieren von Agent-Richtlinien 288
Konfigurieren von Wartungsfensterrichtlinien 292
Lokale Einstellungen 290
manuell zum Standort zuweisen 141
manuelle Deinstallation 286

Manuelle Installation 250, 266
Manuelle Pull-Installation 258
Methoden zum Deinstallieren 280
Paket 286
Siehe auch Symantec Management-Agent-Paket
Parameter des Installationspakets 544
Problemlösung 533
Push-Installation auf Windows Computern 256
Upgrade-Richtlinie 280, 406
verteilen 189
Wartungsfenster 292
Ziel-Einstellungen 290
Symantec Management-Agent für UNIX, Linux und Mac
CSV-Vorlagendatei 268
Deinstallationsrichtlinie 280
Erstellen einer CSV-Datei für Computerdetails 268
Gleichzeitige Installationsaufgaben festlegen 272
Info 246
Installationsanforderungen 269
Installationseinstellungen angeben 271
Installationsmethoden 248
Installationsstatusbericht 260
Installieren auf ausgewählten Computern 272
Manuelle Installation 266
manuelle Pull-Installation 276
Paket 286
Siehe auch Symantec Management-Agent-Paket
Push-Installation auf Computern 272
Upgrade-Richtlinie 280
Voraussetzungen 269
Symantec Management-Agent für Windows
Computer aus CSV-Datei importieren 256
Computer für Installation auswählen 256
Symantec Management-Agent-Paket
konfigurieren 286
Verteilungspunkte aktualisieren 286
Symantec Management-Plattform
Einleitung 23
Info 23, 27
Komponenten 27
Sicherheit 86, 88, 114
Symantec Management-Plattform 7.5
Neue Funktionen 24

T

Task Management
Info 426
Task Server
Bereitstellen 437
Einstellungen 451
Skalieren 437
Tickle 429
Task Service
Einstellungen konfigurieren 146
Tickle
Task Server 429

U

Übersichtsdaten aktualisieren
Hierarchieberichte 178

V

Verbindungsprofil
Erstellen 223
Info 223
Versionshinweise 30
Virtuelle Datenklasse
Erstellen 507
Voraussetzungen
Symantec Management-Agent für UNIX, Linux und Mac installieren 269

W

Wartungsfenster
Anzeigen auf internem Zeitplankalender 130
Konfigurieren von Richtlinien 292
Web-Part
ändern 62
aus Bericht erstellen 469
Berichtergebnisse anzeigen 62
erstellen 62
feste Höhe festlegen 62
Info, auf Portalseiten verwenden 59
Standardgröße festlegen 62
URL anzeigen 62
zur Portalseite hinzufügen 59

X

XML-Datei
Berichtergebnisse speichern 466
Konsolenelemente exportieren 63

Konsolenelemente wiederherstellen 63
Konsolenmenü importieren 54
Konsolenmenü speichern 54
Konsolenuntermenü importieren 54
Speichern von Konsolenelementen 63

Z

Zeichenfolge
Operatoren 575
Zeitplan
Agent-Aufgabe 124
Agent-Richtlinie 125
Aktiver Datumsbereich 129
Aktiver Zeitraum 125
Anzeigen des Notification Server-Zeitplankalenders 130
Auslöser 125
Benutzerdefiniert 125
einschließlich mehrerer Zeitpläne 129
Gemeinsam genutzt 125
geplante Symantec Management-Agent-Installation 259
Komponenten 125
Konfigurieren 129
Modifikatoren 125
Ressourcen-Mitgliedschaftsaktualisierungen 384
Serveraufgabe 124
Serverrichtlinie 124
Verwenden in Notification Server 123
Wartungsfenster 125
Zeitzone 125
Zeitplan-Editor
Öffnen 128
Verwenden 129
Zertifikat
auf verwalteten Computer anwenden 305
von Notification Server exportieren 305
Ziel
abhängig von Filter 382
ändern 398
Automatisch erstelltes Ziel speichern 399
automatisch generiertes Ziel, Info 383, 396
benanntes Ziel, auswählen 403
benanntes Ziel, Info 383, 396
benanntes Ziel, öffnen 400
benanntes Ziel, speichern 401
Benutzer auswählen 399
Computer auswählen 399
Elemente ausschließen 401
Elemente einschließen 401
für Richtlinie festlegen 396
Gruppen von Zielen 403
Info 383
Regeln filtern 401
Ressourcen auswählen 399
Zeitplan aktualisieren 384